F-Secure Anti-Virus Linux Client Security

Administrator’s Guide

"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

This product may be covered by one or more F-Secure patents, including the following:

GB2353372 GB2366691 GB2366692 GB2366693 GB2367933 GB2368233 GB2374260

Copyright © 2007 F-Secure Corporation. All rights reserved. 12000074-07B27

Contents

Chapter 1 Introduction 5

1.1 Welcome 6
1.2 How the Product Works 6
1.3 Key Features and Benefits 9
1.4 F-Secure Anti-Virus Server and Gateway Products 11

Chapter 2 Deployment 13

2.1 Deployment on Multiple Stand-alone Linux Workstations 14
2.2 Deployment on Multiple Centrally Managed Linux Workstations 14
2.3 Central Deployment Using Image Files 15

Chapter 3 Installation 16

3.1 System Requirements 17
3.2 Installation Instructions 18
3.2.1 Stand-alone Installation 19
3.2.2 Centrally Managed Installation 21
3.3 Upgrading from a Previous Product Version 24
3.4 Upgrading the Evaluation Version 25
3.5 Replicating Software Using Image Files 26
3.6 Preparing for Custom Installation 26
3.7 Unattended Installation 27
3.8 Installing Command Line Scanner Only 28
3.9 Creating a Backup 29

3.10 Uninstallation 30

Chapter 4 Getting Started 31

4.1 Accessing the Web User Interface 32
4.2 Basics of Using F-Secure Policy Manager 32
4.3 Testing the Antivirus Protection 33

Chapter 5 User Interface - Basic Mode 34

5.1 Summary 35
5.2 Common Tasks 36

Chapter 6 User Interface - Advanced Mode 37

6.1 Alerts 38
6.2 Virus Protection 40
6.2.1 Real-Time Scanning 40
6.2.2 Scheduled Scanning 44
6.2.3 Manual Scanning 44
6.3 Firewall Protection 49
6.3.1 General Settings 51
6.3.2 Firewall Rules 52
6.3.3 Network Services 54
6.4 Integrity Checking 57
6.4.1 Known Files 57
6.4.2 Verify Baseline 61
6.4.3 Generate Baseline 61
6.4.4 Rootkit Prevention 63
6.5 General Settings 64
6.5.1 Communications 64
6.5.2 Automatic Updates 66
6.5.3 About 69

Chapter 7 Command Line Tools 70

7.1 Overview 71
7.2 Virus Protection 71
7.2.1 fsav 71

7.2.2 dbupdate ... 72
7.3 Firewall Protection ... 72
7.3.1 fsfwc ... 73
7.4 Integrity Checking ... 73
7.4.1 fsic ... 73
7.4.2 fsims ... 74
7.5 General Command Line Tools ... 74
7.5.1 fssetlanguage ... 74
7.5.2 fsma ... 75
7.5.3 fsav-config ... 76

Appendix A Installation Prerequisites 77

A.1 All 64-bit Distributions ... 78
A.2 Red Hat Enterprise Linux 4 ... 78
A.3 Debian 3.1 and Ubuntu 5.04, 5.10, 6.06 ... 79
A.4 SuSE ... 80
A.5 Turbolinux 10 ... 80

Appendix B Installing Required Kernel Modules Manually 81

B.1 Introduction ... 82
B.2 Before Installing Required Kernel Modules ... 82
B.3 Installation Instructions ... 82

Appendix C List of Used System Resources 84

C.1 Overview ... 85
C.2 Installed Files ... 85
C.3 Network Resources ... 85
C.4 Memory ... 86
C.5 CPU ... 86

Appendix D Troubleshooting 87

D.1 User Interface ... 88
D.2 F-Secure Policy Manager ... 89

D.3 Integrity Checking 89
D.4 Firewall 91
D.5 Virus Protection 93
D.6 Generic Issues 93

Appendix E Man Pages 96

Technical Support 165

Introduction 166
F-Secure Online Support Resources 166
Web Club 167
Virus Descriptions on the Web 167

1 INTRODUCTION

Welcome 6
How the Product Works 6
Key Features and Benefits 9
F-Secure Anti-Virus Server and Gateway Products 11

1.1 Welcome

Welcome to F-Secure Anti-Virus Linux Server Security.

Computer viruses are one of the most harmful threats to the security of data on computers. Viruses have increased in number from just a handful a few years ago to many thousands today. While some viruses are harmless pranks, other viruses can destroy data and pose a real threat.

The product provides an integrated, out-of-the-box ready security solution with a strong real-time antivirus protection and a host intrusion prevention (HIPS) functionality that provides protection against unauthorized connection attempts from network, unauthorized system modifications, userspace and kernel rootkits. The solution can be easily deployed and managed either using the local graphical user interface or F-Secure Policy Manager.

F-Secure Policy Manager provides a tightly integrated infrastructure for defining and distributing security policies and monitoring the security of different applications from one central location.

1.2 How the Product Works

The product detects and prevents intrusions and protects against malware. With the default settings, workstations and servers are protected right after the installation without any time spent configuring the product.

Protection Against Malware

The product protects the system against viruses and potentially malicious files.

When user downloads a file from the Internet, for example by clicking a link in an e-mail message, the file is scanned when the user tries to open it. If the file is infected, the product protects the system against the malware.

Real-time Scanning

Real-time scanning gives you continuous protection against viruses as files are opened, copied, and downloaded from the Web. Real-time scanning functions transparently in the background, looking for viruses whenever you access files on the hard disk, diskettes, or network drives. If you try to access an infected file, the real-time protection automatically stops the virus from executing.

Manual Scanning And Scheduled Scanning

When the real-time scanning has been configured to scan a limited set of files, the manual scanning can be used to scan the full system or you can use the scheduled scanning to scan the full system at regular intervals.

Automatic Updates

Automatic Updates keep the virus definitions always up-to-date. The virus definition databases are updated automatically after the product has been installed. The virus definitions updates are signed by the F-Secure Anti-Virus Research Team.

Host Intrusion Prevention System

The Host Intrusion Prevention System (HIPS) detects any malicious activity on the host, protecting the system on many levels.

Integrity Checking

Integrity Checking protects the system against unauthorized modifications. It is based on the concept of a known good configuration - the product should be installed before the server or workstation is connected to the network to guarantee that the system is in a known good configuration.

You can create a baseline of the system files you want to protect and block modification attempts of protected files for all users.

Firewall

The firewall component is a stateful packet filtering firewall which is based on Netfilter and Iptables. It protects computers against unauthorized connection attempts. You can use predefined security profiles which are tailored for common use cases to select the traffic you want to allow and deny.

Protection Against Unauthorized System Modifications

If an attacker gains a shell access to the system and tries to add a user account to login to the system later, Host Intrusion Prevention System (HIPS) detects modified system files and alerts the administrator.

Protection Against Userspace Rootkits

If an attacker has gained an access to the system and tries to install a userspace rootkit by replacing various system utilities, HIPS detects modified system files and alerts the administrator.

Protection Against Kernel Rootkits

If an attacker has gained an access to the system and tries to install a kernel rootkit by loading a kernel module for example through */sbin/insmod* or */sbin/modprobe*, HIPS detects the attempt, prevents the unknown kernel module from loading and alerts the administrator.

If an attacker has gained an access to the system and tries to install a kernel rootkit by modifying the running kernel directly via */dev/kmem*, HIPS detects the attempt, prevents write attempts and alerts the administrator.

1.3 Key Features and Benefits

Superior Protection against Viruses and Worms

- The product scans files on any Linux-supported file system. This is the optimum solution for computers that run several different operating systems with a multi-boot utility.
- Superior detection rate with multiple scanning engines.
- A heuristic scanning engine can detect suspicious, potentially malicious files.
- The product can be configured so that the users cannot bypass the protection.
- Files are scanned for viruses when they are opened and before they are executed.
- You can specify what files to scan, how to scan them, what action to take when malicious content is found and how to alert about the infections.
- Recursive scanning of archive files.
- Virus definition database updates are signed for security.
- Integrated firewall component with predefined security levels. Each security level comprises a set of rules that allow or deny network traffic based on the protocols used.

Transparent to End-users

- The product has an easy-to-use user interface.
- The product works totally transparently to the end users.
- Virus definition databases are updated automatically without any need for end-user intervention.

Protection of Critical System Files

- Critical information of system files is stored and automatically checked before access is allowed.
- The administrator can protect files against changes so that it is not possible to install, for example, a trojan version.
- The administrator can define that all Linux kernel modules are verified before the modules are allowed to be loaded.
- An alert is sent to the administrator when a modified system file is found.

Easy to Deploy and Administer

- The default settings apply in most systems and the product can be taken into use without any additional configuration.
- Security policies can be configured and distributed from one central location.

Extensive Alerting Options

- The product has extensive monitoring and alerting functions that can be used to notify any administrator in the company network about any infected content that has been found.
- Alerts can be forwarded to F-Secure Policy Manager Console, e-mail and syslog.

1.4 F-Secure Anti-Virus Server and Gateway Products

The F-Secure Anti-Virus product line consists of workstation, file server, mail server and gateway products.

- **F-Secure Messaging Security Gateway** delivers the industry's most complete and effective security for e-mail. It combines a robust, enterprise-class messaging platform with perimeter security, antispam, antivirus, secure messaging and outbound content security capabilities in an easy-to-deploy, hardened appliance.
- **F-Secure Internet Gatekeeper for Linux** is a high performance, totally automated web (HTTP and FTP) and e-mail (SMTP and POP) virus scanning solution for the gateway level. F-Secure Internet Gatekeeper works independently of firewall and e-mail server solutions, and does not affect their performance.
- **F-Secure Internet Gatekeeper** (for Windows) is a high performance, totally automated web (HTTP and FTP-over-HTTP) and e-mail (SMTP) virus scanning solution for the gateway level. F-Secure Internet Gatekeeper works independently of firewall and e-mail server solutions, and does not affect their performance.
- **F-Secure Anti-Virus for Microsoft Exchange** protects your Microsoft Exchange users from malicious code contained within files they receive in mail messages and documents they open from shared databases. Malicious code is also stopped in outbound messages and in notes being posted on Public Folders. The product operates transparently and scans files in the Exchange Server Information Store in real-time. Manual and scheduled scanning of user mailboxes and Public Folders is also supported.

- **F-Secure Anti-Virus for MIMEsweeper** provides a powerful anti-virus scanning solution that tightly integrates with Clearswift MAILsweeper and WEBsweeper products. F-Secure provides top-class anti-virus software with fast and simple integration to Clearswift MIMEsweeper for SMTP and MIMEsweeper for Web, giving the corporation the powerful combination of complete content security.
- **F-Secure Anti-Virus for Citrix Servers** ensures business continuity without disruptions caused by viruses and other malicious content. Citrix solutions enable businesses to improve their productivity by providing easy access to information and applications regardless of time, place and access device.

2 DEPLOYMENT

Deployment on Multiple Stand-alone Linux Workstations 14
Deployment on Multiple Centrally Managed Linux Workstations 14
Central Deployment Using Image Files 15

2.1 Deployment on Multiple Stand-alone Linux Workstations

When the company has multiple Linux workstations deployed, but they are not managed centrally, the workstation users can install the software themselves.

- In organizations with few Linux machines, the graphical user interface can be used to manage Linux workstations instead of F-Secure Policy Manager. For more information on stand-alone installation without F-Secure Policy Manager, see "*Stand-alone Installation*"*, 19*.
- Centrally Managed installation with F-Secure Policy Manager installed on a separate computer is recommended. In this mode, F-Secure Policy Manager is used to manage Linux workstations. For more information on Centrally Managed installation, see "*Centrally Managed Installation*"*, 21*.

  The recommended deployment method is to delegate the installation responsibility to each workstation user and then monitor the installation progress via F-Secure Policy Manager Console. After the installation on a host has completed, the host sends an autoregistration request to F-Secure Policy Manager. You can monitor with F-Secure Policy Manager Console which of the hosts have sent an autoregistration request.

2.2 Deployment on Multiple Centrally Managed Linux Workstations

When the company has multiple Linux workstations deployed and they are managed through Red Hat network, Ximian Red Carpet, or similar, the software can be pushed to workstations using the existing management framework.

2.3 Central Deployment Using Image Files

When the company has a centralized IT department that install and maintains computers, the software can be installed centrally to all workstations.

The recommended way to deploy the products is to create an image of a Linux workstation with the product preinstalled. For instructions on how to do this, see “*Replicating Software Using Image Files*”, *26*.

3 INSTALLATION

System Requirements 17
Installation Instructions 18
Upgrading from a Previous Product Version 24
Upgrading the Evaluation Version 25
Replicating Software Using Image Files 26
Preparing for Custom Installation 26
Creating a Backup 29
Uninstallation 30

3.1 System Requirements

Operating system:	› Novell Linux Desktop 9 › SUSE Linux 9.0, 9.1, 9.2, 9.3, 10, 10.1, 10.2 › Ubuntu 5.10 (Breezy), 6.06 (Dapper Drake) › SUSE Linux Enterprise Server 8, 9, 10 › SUSE Linux Enterprise Desktop 10 › Red Hat Enterprise Linux 4, 3, 2.1 AS › Miracle Linux 2.1 › Miracle Linux 3.0 › Asianux 2.0 › Turbolinux 10 › Debian 3.1 The following 64-bit (AMD64/EM64T) distributions are supported with 32-bit compatibility packages: › SUSE Linux Enterprise Server 9, 10 › SUSE Linux Enterprise Desktop 10 › Red Hat Enterprise Linux 4 › Asianux 2.0 › Turbolinux 10
Kernel version:	Linux kernel 2.4 or later (for 64-bit support, Linux kernel 2.6 or later)
Glibc version	Glibc 2.2.4 or later
Processor:	Intel x86
Memory:	256 MB RAM or more
Disk space:	200 MB

Konqueror is not a supported browser with the local user interface. It is recommended to use Mozilla or Firefox browsers.

Note About Dazuko Version

The product needs the Dazuko kernel module for the real-time virus protection, integrity checking and rootkit protection. Dazuko is an open-source kernel module that provides an interface for the file access control. More information is at http://www.dazuko.org.

The product installs the Dazuko driver during the product installation.

The product has been tested extensively with the Dazuko version that is included with the product. Operation with other Dazuko versions or Linux distribution provided Dazuko versions is not supported or recommended.

3.2 Installation Instructions

The following installation modes are available:

- Stand-alone installation.

  This installation mode is meant for evaluation use and for environments with few Linux workstations or servers where central administration with F-Secure Policy Manager is not necessary.

  When you install the product in stand-alone mode you configure and manage the product with the web user interface that can be opened from the system tray, or with the http://localhost:28080/ (local) or https://<host.domain>:28082/ (remote) address.

  In addition to the user interface, the stand-alone installation creates the F-Icon and a program entry under the applications menu, and enables you to use the “right-mouse click” function.

  For installation instructions, see “*Stand-alone Installation*”*, 19*.

- Centrally Managed installation.

  The product is installed locally, and it is managed with F-Secure Policy Manager that is installed on a separate computer.

Centrally managed installation is the recommended installation mode when taking the product into use in a large network environment.

For installation instructions, see "*Centrally Managed Installation*", *21*.

- For information on how to install the product on multiple computers, see "*Replicating Software Using Image Files*", *26*.
- For information on how to install the product in the unattended mode, which does not ask any questions during the installation, see "*Unattended Installation*", *27*.

IMPORTANT: *If you have some other vendor's antivirus software installed on the computer, you must uninstall it before installing the product.*

3.2.1 Stand-alone Installation

During the installation, you must have a compiler and the kernel source installed. Read the documentation of your distribution on how to check that the required tools are installed. For some common distribution-specific instructions how to install required tools to the computer, see "*Installation Prerequisites*", *77*.

It is recommended to use the default settings during the installation. To select the default value, press ENTER to any question during the installation.

Follow these instructions to install the product in stand-alone mode. You will need to install the product using an account with root privileges.

1. Copy the installation file to your hard disk. Use the following command to extract the installation file:

   ```
   tar zxvf f-secure-linux-client-security-<version>.<build>.tgz
   ```
2. Make sure that the installation file is executable:

   ```
   chmod a+x f-secure-linux-client-security-<version>.<build>
   ```
3. Run the following command to start the installation:

   ```
   ./f-secure-linux-client-security-<version>.<build>
   ```

4. Select the language you want to use in the web user interface during the installation.

   ```
   Select language to use in Web User Interface
   [1] English (default)
   [2] Japanese
   [3] German
   ```

5. The installation displays the license agreement. If you accept the agreement, answer yes press ENTER to continue.
6. Enter the keycode to install the full, licensed version of the product. Enter the keycode in the format you received it, including the hyphens that separate sequences of letters and digits:

   If you are installing the evaluation version and do not have a keycode, press ENTER.
7. Select the Standalone installation.
8. Select whether you want to allow the remote access to the web user interface.

   ```
   Allow remote access to the web user interface? [no]
   ```

9. Select whether the web user interface can be opened from the localhost without a login.

   ```
   Allow connections from localhost to the web user interface
   without login? [yes]
   ```

10. Enter the user name who is allowed to access the web user interface.

    ```
    Please enter the user name who is allowed to use the web user
    interface.
    ```

    The user name is a local Linux account. You have to create the account if it does not exist yet. Do not use the root account for this purpose.

11. Select whether you want add currently installed kernel modules to the Integrity Checker known files list and generate the baseline. For more information, see “*Generate Baseline*”, *61*

    ```
    Would you like to enable Linux kernel module verification
    [yes]?
    ```

12. Enter the baseline passphrase. For more information, see "*Passphrase*", *62*.

    `Please insert passphrase for HMAC creation (max 80 characters)`

13. The installation is complete.

After the installation is complete, you can start the F-icon systray applet with the `fsui` command.

For information how to access the web user interface and to see that the virus protection is working, see "*Getting Started*", *31*.

3.2.2 Centrally Managed Installation

During the installation, you must have a compiler and the kernel source installed. Read the documentation of your distribution on how to check that the required tools are installed. For some common distribution-specific instructions how to install required tools to the computer, see "*Installation Prerequisites*", *77*.

When you install the product in centrally managed mode, you must first have F-Secure Policy Manager installed on a separate computer. For F-Secure Policy Manager Console installation instructions, see the F-Secure Policy Manager Administrator's Guide.

IMPORTANT: *Before you start the installation, you have to copy the admin.pub key from F-Secure Policy Manager to the computer where you will install the product. You can do this by using, for example, scp, sftp or any removable media. By default the installation script assumes that the admin.pub key is located in the /root directory.*

Follow the instructions below to install the product in centrally managed mode. You will need to install the product using an account with root privileges.

1. Copy the installation file to your hard disk. Use the following command to extract the installation file:

   `tar zxvf f-secure-linux-client-security-<version>.<build>.tgz`

2. Make sure that the installation file is executable:

```
chmod a+x f-secure-linux-client-security-<version>.<build>
```

3. Run the following command to start the installation:

   ```
   ./f-secure-linux-client-security-<version>.<build>
   ```

   The setup script will display some questions. The default value is shown in brackets after the question. Press ENTER to select the default value.

4. Select the language you want to use in the web user interface during the installation.

   ```
   Select language to use in Web User Interface
   [1] English (default)
   [2] Japanese
   [3] German
   ```

5. The installation displays the license agreement. If you accept the agreement, answer `yes` and press ENTER to continue.

6. Enter the keycode to install the full, licensed version of the product. Enter the keycode in the format you received it, including the hyphens that separate sequences of letters and digits:

   If you are installing the evaluation version and do not have a keycode, press ENTER.

7. Type `C` to select the centrally managed installation.

8. Enter the address of the F-Secure Policy Manager Server.

   ```
   Address of F-Secure Policy Manager Server:
   [http://localhost/]:
   ```

9. Enter the location of the *admin.pub* key. This is the key that you created during F-Secure Policy Manager Console Installation.

   ```
   Give the admin.pub file location [/root/admin.pub]:
   ```

   You can use the TAB *key to complete directory and file names when you enter the file name.*

10. Select whether you want to allow remote accesses to the web user interface.

    ```
    Allow remote access to the web user interface? [no]
    ```

11. Select whether the web user interface can be opened from the localhost without a login.

    `Allow connections from localhost to the web user interface without login? [yes]`

12. Enter the user name who is allowed to use the web user interface.

    `Please enter the user name who is allowed to use the web user interface.`

    The user name is a local Linux account. You have to create the account if it does not exist yet. Do not use the root account for this purpose.

13. Select whether you want add currently installed kernel modules to the Integrity Checker known files list and generate the baseline. For more information, see "*Generate Baseline*", *61*

    `Would you like to enable Linux kernel module verification [yes]?`

14. Enter the baseline passphrase. For more information, see "*Passphrase*", *62*.

    `Please insert passphrase for HMAC creation (max 80 characters)`

15. The installation is complete.
16. Install the included upgrade for F-Secure Policy Manager Console.
    a. Select *Installation Packages* in the *Tools* menu.
    b. Select to import the *fsav_linux_*_mib.jar* file.
17. The product receives the policy file from the F-Secure Policy Manager within 10 minutes after the installation. If you do not want to wait for the policy file, run the following command:

    `/etc/init.d/fsma fetch`

After the installation is complete, you can start the F-icon systray applet with the `fsui` command.

For information how to access the web user interface and to see that the virus protection is working, see "*Getting Started*", *31*.

3.3 Upgrading from a Previous Product Version

If you are running version 5.20 or later, you can install the new version without uninstalling the previous version.

If you have an earlier version, upgrade it to 5.20 first, or uninstall it before you install the latest version. The uninstallation preserves all settings and the host identity, so you do not need to import the host to the F-Secure Policy Manager again. For more information, see “*Uninstalling Earlier Version*”, *25*.

The product upgrade asks for the keycode you have received with the new version. If you are running an earlier version in the evaluation mode, you have to provide a valid keycode for the new version during the upgrade.

If you are running an earlier version in the evaluation mode and you want to evaluate the latest version, you have to uninstall the earlier version first. You can install the latest in the evaluation mode during the clean install.

If you do not have a valid keycode during the upgrade, press CTRL-C to abort the upgrade. The installer uninstalls the product and you can make a clean install.

Manual scanning, scheduled scanning and database update settings have changed in version 5.30 and later. If you have modified these settings before the upgrade, you have to make the same modifications again after the upgrade.

Note that the upgrade deletes all alerts generated with the earlier version.

Upgrading from F-Secure Anti-Virus 4.65

You can upgrade version 4.65 to a command line only installation of version 5.52 by running the installer normally. Your old configuration file will be stored as */opt/f-secure/fsav/migration/fsav4.conf*. For more information, see “*Installation Instructions*”, *18*.

If you want to upgrade version 4.65 to the full 5.52 version, uninstall the old version first and run 5.52 installer normally. For more information, see “*Uninstalling Earlier Version*”, *25*.

Uninstalling Earlier Version

If you have version 5.x, run the following command from the command line to uninstall it

```
/opt/f-secure/fsav/bin/uninstall-fsav.
```

If you have version 4.x, remove the following directories and files to uninstall it:

```
/opt/f-secure/fsav/
/var/opt/f-secure/fsav/
/etc/opt/f-secure/fsav/
/usr/bin/fsav
/usr/share/man/man1/fsav.1
/usr/share/man/man5/fsav.conf.5
/usr/share/man/man5/fsavd.conf.5
/usr/share/man/man8/dbupdate.8
/usr/share/man/man8/fsavd.8
/usr/share/man/man8/fsavschedule.8
```

3.4 Upgrading the Evaluation Version

If you want to upgrade the evaluation version to the full, licensed version of the product, run the installation as normal. The upgrade script will notice the trial version and upgrades the packages.

Enter the keycode to upgrade to the licensed version of the product. Enter the keycode in the format you received it, including the hyphens that separate sequences of letters and digits.

If the evaluation period has expired, uninstall the current installation first. For more information, see “Uninstallation”, 30.

3.5 Replicating Software Using Image Files

If you are going to install the product on several computers, you can create a disk image file that includes the product and use this image to replicate the software on the computers. Make sure that each computer on which the software is installed will create a new unique identification code.

Follow these steps to make sure that each computer uses a personalized Unique ID when a disk imaging software is used:

1. Install the system and all the software that should be in the image file, including the product.
2. Configure the product to use the correct F-Secure Policy Manager Server. However, do not import the host to F-Secure Policy Manager Console if the host has sent an autoregistration request to the F-Secure Policy Manager Server. Only hosts on which the image file will be installed should be imported.
3. Run the command following command:

   ```
   /etc/init.d/fsma clearuid
   ```

   The utility program resets the Unique ID in the product installation.
4. Shut down the computer and do not restart the computer before the image file has been created.
5. Create the disk image file.

A new Unique ID is created automatically when the system is restarted. This will happen individually on each machine where the image file is installed. These machines will send autoregistration requests to F-Secure Policy Manager and the request can be processed normally.

3.6 Preparing for Custom Installation

The product installation package is a self extracting package, which contains the software as RPMs. If there is a need to create a custom installation package, the RPMs can be extracted from the package as follows:

1. Type the following command:

   ```
   ./f-secure-linux-client-security-<version>.<build> rpm
   ```

2. Install RPM packages.

IMPORTANT: *The /opt/f-secure/fsav/fsav-config script must be executed after the RPMs have been installed, otherwise the product will not operate.*

3.7 Unattended Installation

You can install the product in the unattended mode. In unattended mode, you provide all the information on the installer command line (or `fsav-config` command line, if you install from RPM packages). The unattended installation mode asks no questions during the installation.

Use the following command line switch during the installation:

```
--auto MODE [fspms=FSPMSURL adminkey=/PATH/TO/ADMIN.PUB]
lang=en|de|ja [no]remotewui [no]locallogin user=USER
kernelverify|nokernelverify pass=PASSPHRASE keycode=KEYCODE
```

Where `MODE` is `standalone` for the standalone installation or `managed` for the centrally managed installation.

If `MODE` is `managed`, you have to provide the URL to F-Secure Policy Manager Server and the location of the administrator public key, for example: *fspms=http://fspms.company.com/ adminkey=/root/admin.pub*

Use the following options in the command line:

lang	Select the language for the web user interface.
remotewui	Allow remote access to the web user interface.
noremotewui	Do not allow remote access to the web user interface.
nolocallogin	Allow local access to the web user interface without login.

locallogin	Require login for the local access to the web user interface.
user=USER	Specify the local account to use for the web user interface login.
kernelverify	Turn on the kernel module verification.
nokernelverify	Turn off the kernel module verification.
pass=PASS	Specify the passphrase for the baseline generation.
keycode=KEYCODE	Specify the keycode for license checks. If no keycode is provided, the product is installed in the evaluation mode.

For example, to install the product in standalone mode with English web user interface, with no remote access to user interface and not requiring login for local user interface access and not using kernel module verification:

```
./f-secure-linux-client-security-<version>.<build> --auto
standalone lang=en noremotewui nolocallogin nokernelverify
```

3.8 Installing Command Line Scanner Only

The command line only installation installs only the command line scanner and the automatic update agent. The installation mode is designed for users migrating from F-Secure Anti-Virus for Linux 4.6x series and for users who do not need the real-time protection, integrity checking, web user interface or central management, for example users running AMaViS mail virus scanner.

Use the following command line when running the installer to install the command line scanner only version of the product:

```
./f-secure-linux-server-security-<version>.<build>
--command-line-only
```

If you are running an earlier version and you want to upgrade to the latest version, but you want to install the command line scanner only, you have to uninstall the earlier version first.

Use the */etc/opt/f-secure/fssp/fssp.conf* configuration file to configure the command line scanner only installation. See the file for detailed descriptions of the available settings.

3.9 Creating a Backup

To backup all relevant data, run the following commands:

```
# /etc/init.d/fsma stop
# /etc/init.d/fsaua stop
# tar cpsf <backup-filename>.tar /etc/init.d/fsma /etc/
init.d/fsaua /etc/opt/f-secure /var/opt/f-secure /opt/
f-secure
# /etc/init.d/fsaua start
# /etc/init.d/fsma start
```

To restore data from backup file, run the following commands:

```
# /etc/init.d/fsma stop
# /etc/init.d/fsaua stop
# cd /
# rm -rf /var/opt/f-secure
# tar xpsf <backup-filename>.tar
# /etc/init.d/fsaua start
# /etc/init.d/fsma start
```

Make sure that *fsma* and *fsaua* users and fsc group exist after the backup has been restored, for exampe by backing up also */etc/passwd*, */etc/shadow* and */etc/group* files.

3.10 Uninstallation

Run the script `/opt/f-secure/fsav/bin/uninstall-fsav` as root to uninstall the product.

The uninstall script does not remove configuration files. If you are sure that you do not need them any more, remove all files in the */etc/opt/f-secure/fsma* path.

4 GETTING STARTED

Accessing the Web User Interface 32
Basics of Using F-Secure Policy Manager 32
Testing the Antivirus Protection 33

4.1 Accessing the Web User Interface

In small deployments where F-Secure Policy Manager is not available, the web user interface can be used to configure the product. You can access the web user interface from the system tray, or with the http://localhost:28080/ address.

If you allow the remote access to the web user interface, you can access it with the following HTTPS address: https://<host.domain>:28082/.

It is possible to have in use both F-Secure Policy Manager and the web user interface at the same time. Note that the user can locally override the settings created with F-Secure Policy Manager unless the administrator has prevented this by selecting the *Final* checkbox in the F-Secure Policy Manager settings.

4.2 Basics of Using F-Secure Policy Manager

If your corporate network utilizes F-Secure Policy Manager to configure and manage F-Secure products, you can add the product to the existing F-Secure Policy Manager environment. In the centralized administration mode, F-Secure Policy Manager Console is used to change settings and view statistics of the F-Secure products.

Use the variables under the *F-Secure Anti-Virus Linux Server Security / Settings* branch or *F-Secure Anti-Virus Linux Client Security / Settings* to define settings for the product. depending on the installed product.

For more information about F-Secure Policy Manager, see F-Secure Policy Manager Administrator's Guide.

4.3 Testing the Antivirus Protection

To test whether the product operates correctly, you can use a special test file that is detected as a virus. This file, known as the EICAR Standard Anti-Virus Test File, is also detected by several other anti-virus programs. You can use the EICAR test file also to test your E-mail Scanning. EICAR is the European Institute of Computer Anti-virus Research. The Eicar info page can be found at
http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml

You can test your antivirus protection as follows:

1. You can download the EICAR test file from
   http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml

   Alternatively, use any text editor to create the *eicar.com* file with the following single line in it:

   ```
   X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```
2. Run the following command:
   fsav *eicar.com*
3. The product should detect the file as a virus. Naturally, the file is not a virus.

5 User Interface - Basic Mode

Summary 35
Common Tasks 36

5.1 Summary

The summary page displays the product status and the latest reports. The product status displays the protection status and any possible errors or malfunctions.

Status

Virus Protection	Shows the current Virus Protection level. Virus Protection levels allow you to change the level of protection according to your needs. If Virus Protection is disabled, your computer is vulnerable to virus attacks.
Firewall Protection	Shows the current firewall protection level. The firewall protection levels allow you to instantly change your firewall rule set. For more information, see “*Firewall Rules*”, *52*. If Firewall Protection is disabled, your computer is vulnerable to hacking attacks.
Integrity Protection	Shows the current integrity protection level. For more information, see “*Integrity Checking*”, *57*. If Integrity Protection is disabled, your computer is vulnerable to rootkits.

Click **Details...** for more information about the current protection status.

Reports

Virus Definitions Updated	Shows the time and status of the latest update.
Alerts	Shows the number of unread security alerts. Click **View** to view a list of alerts. For more information, see“*Alerts*”, *38*.

5.2 Common Tasks

You can configure the manual scan and firewall settings and check the latest virus definition database updates from the common tasks page.

Choose one of the following actions:

Scan the computer for malware	Opens a scanning wizard that can scan the computer for any type of malware, including viruses, worms and trojans. Follow the on-screen instructions for more details. For more information, see "*Manual Scanning*", *44*.
Create a firewall rule	Create a new firewall rule. You can control which type of network traffic is allowed and denied with firewall rules. For more information, see "*Add And Edit Rules*", *53*.
Check the integrity of the file system	Check that important system files have not been modified without permission. For more information, see "*Integrity Checking*", *57*.
Update virus definitions	Retrieve the latest virus definition database updates from the Internet. For more information, see "*Automatic Updates*", *66*.
Install software	Install new software while maintaining the system integrity. The integrity checker checks the full system integrity and reports results, after which you can proceed installing software. Follow the on-screen instructions for more details. For more information, see "*Software Installation Mode*", *60*.

Click **Modify advanced settings...** to view and configure advanced settings.

6 User Interface - Advanced Mode

Alerts 38
Virus Protection 40
Firewall Protection 49
Integrity Checking 57
General Settings 64

6.1 Alerts

On the Alerts page, you can read and delete alert messages. To find the alert message you want to view, follow these instructions:

1. Select the *Status* of security alerts you want to view.
   - Select All to view All alerts.
   - Select Unread to view new alerts.
   - Select Read to view alerts you have already viewed.
2. Select the *Severity* of security alerts you want to view. For more information, see "*Alert Severity Levels*", *38*.

Click alerts to highlight them and click **Mark highlighted as read** to flag them as read messages. Click **Delete highlighted** to delete all highlighted alerts.

Alert Database Maintenance

You can delete or mark multiple messages as read simultaneously. Select how old and which alert severity messages you want to edit and click **Perform action** to delete or mark selected messages as read.

Alert Severity Levels

Alerts are divided into following severity levels:

Security Level	Description
Informational	Normal operating information from the host.
	For example, starting to update virus databases.
Warning	A warning from the host.
	For example, an error when trying to read a file.
Error	Recoverable error on the host.

Security Level	Description
	For example, the virus definition database update is older than the previously accepted version.
Fatal Error	Unrecoverable error on the host that requires attention from the administrator.
	For example, a process fails to start or loading a kernel module fails.
Security alert	For example, a virus-alert. The alert includes information of the infection and the performed operation.

6.2 Virus Protection

- Real-Time Scanning

  Real-time scanning is completely transparent. By default, all files are scanned automatically when they are opened and executed.

- Scheduled Scanning

  If you want to scan the computer for viruses regularly, for example once a week, you can create a scheduled scanning task. Scheduled scanning uses the settings you have defined for manual scanning.

- Manual Scanning

  You can launch a manual scan any time you want if you suspect that there might be a virus on a computer. You can specify the manual scanning settings, for example the directories to scan and the action to take, independently of the real-time scanning settings.

6.2.1 Real-Time Scanning

On the Real-Time Scanning page, you can select what to scan automatically in real-time and what to do when a virus or other malware is found.

In most cases you do not need to change the Real-Time Scanning default settings before you take the system into use.

When the real-time scanning is enabled, any file you open is automatically scanned for viruses.

Action on infection

Select the primary and secondary actions to take when a virus is found. The secondary action takes place if the primary action cannot be performed.

By default, the primary action for infections is *Disinfect* and secondary action *Rename*. Choose one of the following actions:

Report and deny access	Displays and alerts about the found virus and blocks access to it. No other action is taken against the infected file. View *Alerts* to check security alerts. For more information, see "*Alerts*", *38*.
Disinfect	Disinfects viruses. Note that some viruses cannot be disinfected. If the virus cannot be disinfected, the access to the infected file is still blocked.
Rename	Renames the infected file and removes its execute permissions. Renamed infected file stays on the computer, but it cannot cause any damage. The renamed file has *.virus* extension.
Delete	Deletes the infected file.
Deny access	Blocks the access to the infected file, but does not send any alerts or reports.

Suspected files

Select the primary and secondary actions to take when heuristics scanning engine finds a suspected file. The secondary action takes place if the primary action cannot be performed.

By default, the primary action for suspected files is *Report only* and secondary action *Deny access*. Choose one of the following actions:

Report and deny access	Displays and alerts about the suspected file and blocks access to it. No other action is taken. View *Alerts* to check security alerts. For more information, see "*Alerts*", *38*.
Rename	Renames the suspected file and removes its execute permissions. Renamed suspected file stays on the computer, but it cannot cause any damage.

	The renamed file has *.suspected* extension.
Delete	Deletes the suspected file.
Deny access	Blocks the access to the suspected file, but does not send any alerts or reports.
What to scan	
Directories excluded from the scan	Define directories which are excluded from the virus scan. Type each directory on a new line, only one directory per line. If scanning a certain directory takes a long time and you know that no user can create or copy an infected file in it, or you get false alarms during the scan, you can exclude the directory from the virus scan. *The list can also contain files if you want to exclude specific files from the scan.*
Scan only executables	Select whether only executables in scanned directories are scanned for viruses. Clear the check box to scan all files for viruses.
Whitelisted executables	Define executables which may access any files. The real-time virus scan does not block any file accesses from whitelisted executables.
Whitelisted executables must match baseline	Select whether whitelisted executables must be unmodified in the known files list. If this setting is enabled and the executable cannot be found in the integrity checking baseline, is not whitelisted.
Scan when opening a file	Select whether files are scanned every time they are opened.
Scan when closing a file	Select whether files are scanned every time they are closed.

Scan when running an executable	Select whether files are scanned every time they are run.

If Scan on open and Scan on execute are disabled, nothing is scanned even if Scan only executables is enabled.

Archive scanning

Scan inside archives	Scan files inside compressed ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR and TGZ archives.

Scanning archives with the real-time scanning can degrade the overall system performance.

When the archive scanning is enabled, some e-mail clients may stop processing further e-mails when an infected e-mail is opened.

Maximum number of nested archives	Set the number of levels in nested archives the product should scan. Nested archives are archives inside other archives.
Treat password protected archives as safe	Password protected archives cannot be scanned for viruses. Select whether password protected archives are treated as safe and the access to them is allowed or if they are treated as unsafe and the user cannot access the archive. The user who opens the password protected archive should have an up-to-date virus protection on the workstation if password protected archives are treated as safe.
Stop on first infection inside an archive	Select whether the whole archive should be scanned even after an infection is found inside the archive.

6.2.2 Scheduled Scanning

You can use the scheduled scanning to scan files for viruses regularly at predefined times.

To set the scanning schedule, follow these instructions:

1. Click **Add a new task**.
2. Set the date and time when the scheduled scan should start. For example:
   a. To perform the task each sunday at 4 am:

      Minute: 0, Hour: 4, Day of the Month: *, Month: *, Day of the Week: sun

   b. To perform the task every day at 5:30 am:

      Minute: 30, Hour: 5, Day of the Month: *, Month: *, Day of the Week: *
3. Select directories that should be scanned at the scheduled time.
4. Click **Save task** to add the scheduled scanning task into the schedule.

The scheduled scanning tasks use the Manual Scanning settings. For more information, see "*Manual Scanning*", *44*.

A scheduled scan can take several hours, so it is a good idea to run it when the system is idle, for exampe during the night. Another alternative is to configure several scheduled scan tasks, and to scan only some directories at one time.

6.2.3 Manual Scanning

The manual scanning settings are used when you want to scan files or directories for viruses manually and during the scheduled scanning.

If you have received a suspicious file, for example an executable or an archive file via e-mail, it is always a good idea to scan it for viruses manually.

By default, the archive scanning is disabled during the real-time scan. The real-time scan scans the archive when it is extracted, but if you copy or forward the archive without extracting it first, you should manually scan the archive to make sure that it does not contain any viruses.

To start the manual scan, select **I want to... > Scan the computer for malware** in the basic mode. For more information, see "*Common Tasks*", *36*.

Action on infection

Select the primary and secondary actions to take when a virus is found. The secondary action takes place if the primary action cannot be performed.

By default, the primary action for infections is *Disinfect* and secondary action *Rename*. Choose one of the following actions:

Report and deny access	Displays and alerts about the found virus. No other action is taken against the virus. View *Alerts* to check security alerts. For more information, see "*Alerts*", *38*.
Disinfect	Disinfects viruses. Note that some viruses cannot be disinfected.
Rename	Renames the infected file removes its execute permissions when a virus is found. Renamed infected file stays on the computer, but it cannot cause any damage. The renamed file has *.virus* extension.
Delete	Deletes the infected file when a virus is found.

Custom	Performs the action you define. To define the custom action, enter the command to the *Primary* or *Secondary custom action* field.
Deny access	Blocks the access to the infected file, but does not send any alerts or reports.
Abort Scan	Stops the scan.

Suspected files

Select the primary and secondary actions to take when heuristics scanning engine finds a suspected file. The secondary action takes place if the primary action cannot be performed.

By default, the primary action for suspected files is *Report only* and secondary action *Deny access*. Choose one of the following actions:

Report and deny access	Displays and alerts about the suspected file and blocks access to it. No other action is taken. View *Alerts* to check security alerts. For more information, see “*Alerts*”, *38*.
Rename	Renames the suspected file and removes its execute permissions. Renamed suspected file stays on the computer, but it cannot cause any damage. The renamed file has *.suspected* extension.
Delete	Deletes the suspected file.
Deny access	Blocks the access to the suspected file, but does not send any alerts or reports.

What to scan

Scan files	Define files that are scanned during the manual scan. *All files* - Scans all files in the system.

	Only files with specified extensions - Scans only files with the extensions specified in the *Included extensions* field. The *Included extensions* field appears after you have selected *Only files with specified extensions*,
Enable exclusions	Files with the extensions specified in the *Directories excluded from scanning* field are not scanned. The *Directories excluded from scanning* field appears after you have enabled exclusions.
Directories excluded from scanning	Define directories which are excluded from the virus scan if the *Enable exclusions* setting is selected. Type each directory on a new line, only one directory per line.
Scan also executables	Scan any executable files in addition to all other specified files during the manual scan.
Archive scanning	
Scan inside archives	Scan files inside compressed ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR and TGZ archives.
Maximum number of nested archives	Set the number of levels in nested archives the product should scan. Nested archives are archives inside other archives.
Treat password protected archives as safe	Password protected archives cannot be scanned for viruses. Select whether password protected archives are treated as safe.

	The user who opens the password protected archive should have an up-to-date virus protection on the workstation if password protected archives are treated as safe.
Stop on first infection inside an archive	Select whether the whole archive should be scanned even after an infection is found inside the archive.

Scanning a File Manually on a Workstation

When the product scans files, it must have at least read access to them. If you want the product to disinfect infected files, it must have write access to the files.

You can scan files manually from the KDE filemanager. Right-click on any file you want to scan and select *Scan* to scan the file for viruses.

Command Line

For information how to scan files from the shell, see “*fsav*”, *71*.

6.3 Firewall Protection

The firewall protects the computers against unauthorized access from the Internet as well as against attacks originating from inside the local-area network. It provides protection against information theft as unauthorized access attempts can be prohibited and detected.

- Security Profiles

  The firewall contains predefined security profiles which have a set of pre-configured firewall rules. Different security profiles can be assigned to different users; for example based on the company security policy, user mobility, location and user experience.

- Firewall Rules

  You can configure the firewall by creating and editing firewall rules. Firewall rules are a set of firewall services - Internet traffic parameters that control which type of traffic is allowed and denied. One rule can contain multiple services.

- Network Services

  Network services are described by what protocol and port they use, for example web browsing uses TCP protocol and the port number 80.

Security Profiles

You can change the current security profile from the Summary page. For more information, see “*Summary*”, *35*.

The following table contains a list of the security profiles available in the product and the type of traffic each of them either allow or deny.

Security profiles	Description
Block All	Blocks all network traffic (excluding loopback).
Server	Allows only IP configuration via DHCP, DNS lookups and ssh protocol out and in. The server profile has to be customized before it can be taken into use.
Mobile	Allows normal web browsing and file retrievals (HTTP, HTTPS, FTP), as well as e-mail and Usenet news traffic. Encryption programs, such as VPN and SSH are also allowed. Everything else is denied. Local rules can be added after the malware probes detection.
Home	Allows all outbound TCP traffic and FTP file retrievals. Everything else is denied. Local rules can be added to enable new network functionality.
Office	Allows all outbound TCP traffic and FTP file retrievals. Everything else is denied by default. With this profile, a firewall should exist between 0.0.0.0/0 and the host.

Security profiles	Description
Strict	Allows outbound web browsing, e-mail and News traffic, encrypted communication, FTP file transfers and remote updates. Everything else is denied.
Normal	Allows all outbound traffic, and denies some specific inbound services.
Disabled	Allows all inbound and outbound network traffic.

6.3.1 General Settings

On the General Settings page, you can select network packet logging settings and configure trusted network interfaces.

Enable firewall	Select the *Enable firewall* check box to enable the firewall protection. Clear the check box to disable the firewall.
Log all unhandled network packets	Select to log all network packets that do not match to any firewall rules. You can log unhandled network packets in problem solving situations. By default, leave the check box deselected.
Trusted network interfaces	Firewall rules are applied to the first network interface on the host and all other interfaces are blocked. If other interfaces are connected to trusted networks, add those interfaces to the list and separate each entry with a comma. All traffic to trusted network interfaces is allowed.

6.3.2 Firewall Rules

Each security profile has a set of pre-configured Firewall Rules.

Profile to edit	Select the firewall profile you want to edit. For more information, see "*Security Profiles*", *50*. The current security profile is displayed on the top of the Firewall Rules page. You can change the current security profile from the Summary page. For more information, see "*Summary*", *35*.
List of rules	The list of rules displays the currently used ruleset. Clear the *Enabled* checkbox to disable the rule temporarily. Use up and down arrows to change the order of rules in the ruleset. The order of the rules is important. The rules are read from top to bottom, and the first rule that applies to a connection attempt is enforced. For example: You have a rule that allows an IRC (Internet Relay Chat) connections to a specific host above a rule that denies all IRC traffic. You are still allowed to make the connection to that one host. However, if the rule that denies all IRC traffic comes first, any other IRC rules below that rule are ignored and no IRC connections can be made. Click **X** to delete the rule permanently. To edit a rule, select it from the list of rules. The selected rule is displayed in the *Edit Rule* pane. The *Edit Rule* pane appears below the list of rules.

If the profile contains more than 10 rules, use **<<**, **<**, **>** and **>>** arrows to browse rules.

Changing the order of the rules may affect all the other rules you have created.

Add And Edit Rules

You can add a new firewall rule, for example, to allow access to a new service in the network.

To add a new rule, click **Add new rule** below the list of rules.

When you edit the firewall rules, you should allow only the needed services and deny all the rest to minimize the security risk.

Type	Choose whether the rule allows or denies the service.
Remote host	Enter details about target addresses. Enter the IP address and the subnet in bit net mask format. For example: 192.168.88.0/29. You can use the following aliases as the target address: `[myNetwork]` - The local-area network. `[myDNS]` - All configured DNS servers.
Description	Enter a short description for the rule.

Services connected to this rule

Service	Select services for which you want the rule to apply. You can add multiple services to each rule. Click **Add Service to this rule** after each service you want to add. Each rule must have at least one service. If the rule contains a new service, make sure you have saved the service list in the Network Services page. For more information, see "*Network Services*", *54*.

Direction	For every service you selected, choose the direction in which the rule applies. *in* = all incoming traffic that comes to your computer from the internet. *out* = all outgoing traffic that originates from your computer.

Click **Add to firewall rules** to add the rule to the end of the list of rules.

Click **Save** after you have added or edited a rule to activate all changes. Click **Cancel** to discard all changes made after the previous save.

6.3.3 Network Services

The Network Services page displays the network services that currently exist in the system. When you want to enable or disable the use of a certain service, you have to make sure that the service exists in the Network Services table. After that you can create a firewall rule that allows or denies the use of that service.

To add a new service, click **Add new service** below the list of services.

To edit a service, select it from the list of services.

Add And Edit Services

Service name	Enter a name for the service.
Protocol	Select the protocol (ICMP, TCP, UDP) or define the protocol number for the service you want to specify.
Initiator ports	Enter initiator ports.
Responder ports	Enter responder ports.
Description	Enter a short description of the service.

Click **Save** after you have added or edited a service to activate all changes. Click **Cancel** to discard all changes made after the previous save.

Creating Firewall Services and Rules

To enable the use of a new service, do the following:

1. Select the *Network Services* in the Advanced mode menu.
2. Define a unique name for the service in the **Service Name** field. You can also enter a descriptive comment in the **Description** field to distinguish this service from other services.
3. Select a protocol number for the service from the **Protocol** drop-down list. If your service does not use ICMP, TCP or UDP protocol, select *Numeric* and type the protocol number in the field reserved for it.
4. If your service uses the TCP or UDP protocol, you need to define **Initiator Ports** the service covers.
5. If your service uses TCP or UDP protocols, you need to define **Responder Ports** the service covers.
6. Click **Add as a new service** to add the service to the Network services list.
7. Click **Save** to save the new service list.

8. The next step is to create a Firewall Rule that allows use of the service you just defined. Select *Firewall Rules* in the Advanced mode menu.
9. Select the profile where you want to add a new rule and click **Add new rule** to create a new rule.
10. Select *Accept* or *Deny* as a rule **Type**. Enter a descriptive comment in the **Description** field to distinguish this rule.
11. Define **Remote Host** to which the rule applies. Enter the IP address of the host in the field.
12. Select the new service you have created in the **Service** field and the direction when the rule is applied.
13. Click **Add Service to This Rule**. If you do not want to add other services to the same rule, click **Add to Firewall Rules** to add the rule to the active set of rules on the Firewall Rules table.
14. Click **Save** to save the new rule list.

6.4 Integrity Checking

Integrity Checking protects important system files against unauthorized modifications. Integrity Checking can block any modification attempts of protected files, regardless of file system permissions.

Integrity Checking compares files on the disk to the baseline, which is a cryptographically signed list of file properties.

Integrity Checking can be configured to send alerts to the administrator about modification attempts of the monitored files. “*Communications*”, *64*.

- Known Files

  The Known Files lists files that the product monitors and protects.
- Verify Baseline

  Verify the system integrity manually.
- Generate Baseline

  Generate a new baseline for all known files.
- Rootkit Prevention

  Adjust rootkit prevention settings.

6.4.1 Known Files

The Known Files lists files that the product monitors and protects. The baseline is created from the Known Files list by reading the properties of the files in the list and cryptographically signing the result. Integrity Checking compares this result to real-time file accesses.

Use the search filters to select files you want to view in the list.

Using The Search

Status	Select files you want to view in the known files list. *Modified and new* - Displays all files that have been modified or added to the baseline. *Modified* - Displays all files that have been modified. *New* - Displays all files that have been added to the baseline. *Unmodified* - Displays all baselined files that have not been modified. *All* - Displays all files in the known files list.
Filename	Enter any part of the filename of the monitored file you want to view in the known files list.

Integrity Checking does not protect new or modified files before you regenerate the baseline. If you add files to the Known Files list or files have been modified, regenerate the baseline to protect those files.

Click **Search** to view the search results.

Filename	Displays the name of the file.
Detection time	Displays the time when a modification was detected.
Detected modifier	Displays the filename of the process that modified the file.

Action	Displays whether the product allows or denies modifications to the file.
Alert	Displays whether the product sends an alert when the file is modified.
Protection	Displays whether the file is monitored or protected. Protected files cannot be modified while monitored files are only monitored and can be modified.

To regenarate the baseline, select new and modified files you want to baseline and click **Regenerate baseline for highlighted files**. For more information, see "*Generate Baseline*"*, 61*.

If you want to remove files from the baseline, click files to select them and click **Remove highlighted files** to stop monitoring the selected files.

Adding Files To The Known Files List

To add a file to the known files list, enter the filename and select the protection method you want to use.

Filename	Enter the filename of the file you want to monitor. If you want to add more than one file, separate each filename with a space.
Protection	Select the protection method: Monitor - Monitors the file but does not prevent any modifications to it. Protect - Does not allow any modifications to the file. The protected file can be opened but it cannot be changed.

Action	The product can prevent the access to modified files. Allow - The access to the modified file is allowed when it is executed or opened. Deny - The access to the modified file is denied. Modified files cannot be opened or executed.

Click **Add to known files** to add the entry to the Known Files List.

Integrity Checking does not protect new or modified files before you regenerate the baseline. Regenerate the baseline to protect files you have added. For more information, see "*Generate Baseline*"*, 61*.

You can add a single file or multiple files to the baseline at the same time.

Software Installation Mode

Integrity Checking prevents unauthorized and unwanted modifications of system files and programs. When you update your operating system, apply a security update or install new versions of software, you need to modify files that Integrity Checking monitors.

Use the Software Installation Mode when you want to modify system files and programs. To access the Software Installation Mode, open the user interface, select *I want to...* and click **Install software**.

The Software Installation Mode wizard guides you through the software installation and updates the baseline with new software that you install on your system.

When the Software Installation Mode is enabled, any process can load any kernel modules regardless whether they are in the baseline or not and any process can change any files in the baseline, whether those files are protected or not. The real-time scanning is still enabled and it alerts of any malware found during the installation.

IMPORTANT: *If you install software without the Software Installation Mode when Integrity Checking monitors updated files, you may be unable to install or use the new software. For example, Integrity Checking may prevent a kernel update from booting properly as new drivers are not in the baseline.*

Command Line

For information how to use the Software Installation Mode from the shell, see “*fsims*”, *74*.

6.4.2 Verify Baseline

Enter your passphrase to verify the baseline. For more information about the passphrase, see “*Passphrase*”, *62*.

Do not start any other integrity checking processes while the product verifies the baseline.

You can verify the baseline manually to make sure that your system is safe and all baselined files are unmodified. If an attacker has managed to gain a root access to the system and regenerated the baseline, the regenerated baseline does not match against your passphrase when you verify the baseline.

6.4.3 Generate Baseline

Integrity Checking is set up by creating a baseline of the system files that you want to protect.

A default set of system files is added to the Known Files list during the installation. By default, Kernel Module Verification is enabled during the installation and the baseline is generated from the Known Files list. If you

do not enable the Kernel Module Verification during the installation, you have to generate the baseline manually before Integrity Checking is enabled.

All files that are added to the baseline during the installation are set to *Allow* and *Alert* protection mode.

Passphrase

The generated baseline has to be signed to prevent anyone from modifying the protected files.

The product verifies the baseline and the system integrity cryptographically. A cryptographic algorithm is applied to the baseline contents and the passphrase to generate a signature (a HMAC signature) of the baselined information.

IMPORTANT: *You must take great care not to forget the passphrase used as it cannot be recovered and the baseline cannot be verified against tampering without using the same passphrase.*

You should not share the passphrase with other administrators without fully understanding the consequences. Other administrators could tamper with the baseline and regenerate it using the same passphrase, and the subsequent check would appear to be all right.

Command Line

For information how to create and check the system integrity from the shell, see “*fsic*”, *73*.

6.4.4 Rootkit Prevention

When the Integrity Checking is enabled, the product can prevent rootkits. Hackers can use rootkits to gain access to the system and obtain administrator-level access to the computer and the network.

Kernel module verification	Protects the system against rootkits by preventing unknown kernel modules from loading. When the kernel module verification is on, only those kernel modules that are listed in the known files list and which have not been modified can be loaded. If the kernel module verification is set to Report only, the product sends an alert when an unknown or modified kernel module is loaded but does not prevent it from loading.
Write protect kernel memory	Protects the */dev/kmem* file against write attempts. A running kernel cannot be directly modified through the device. If the write protection is set to Report only, the product sends an alert when it detects a write attempt to */dev/kmem* file, but it does not prevent the write operation.
Allowed kernel module loaders	Specify programs that are allowed to load kernel modules when the kernel module verification is enabled. By default, the list contains the most common module loaders. If the Linux system you use uses some other module loaders, add them to the list. Type each entry on a new line, only one entry per line.

6.5 General Settings

- Communications
  Configure alerting.
- Automatic Updates
  Configure automatic virus definition database updates.
- About
  View the product and version information.

6.5.1 Communications

Change *Communications* settings to configure where alerts are sent.

Management Server

Server Address	Define the URL of the F-Secure Policy Manager Server address. This setting is only available in the centrally managed installation mode.

Alert Forwarding

Alert Level	Specify where an alert is sent according to its severity level. You can send an alert to any of the following: *E-mail to* - Enter the e-mail address where the alert is sent as an e-mail. *Local* - Alert is displayed in the Web User Interface. *Syslog* - Alert is written to the system log. The syslog facility is LOG_DAEMON and alert priority varies. *FSPMC* - Alert is sent to F-Secure Policy Manager Console.

E-mail Settings

The e-mail settings are used for all alert messages that have been configured to send e-mail alerts.

Server — Enter the address of the SMTP server in the Server Address field. You can use either the DNS-name or IP-address of the SMTP server.

If the mail server is not running or the network is down, it is possible that some e-mail alerts are lost. To prevent this, configure a local mail server to port 25 and use it for relaying e-mail alerts.

From — Enter the full e-mail address (sender@example.com) you want to use as a sender of the alert in the e-mail message.

Subject — Enter the e-mail alert message subject. Use `%DESCRIPTION%` as the subject to display a short description of the alert in the subject line.

Alert Message Variables

The following table lists all variables that are available for the e-mail alert message subject.

Variable	Description
%SEVERITY%	The severity of the alert: informational, warning, error, fatal error or security alert.
%HOST_DNS%	The DNS address of the host that sent the alert.
%HOST_IP%	The IP address of the host that sent the alert.
%USER%	The active user login name.
%PRODUCT_NAME%	The name of the product that generated the alert.

Variable	Description
%PRODUCT_OID%	The OID of the product that generated the alert.
%DESCRIPTION%	The alert description.
%DATE%	The date when an alert sent in format YYYY-MM-DD.
%TIME%	The time when an alert sent in format HH:MM:SS+GMT.
%ALERT_NUMBER%	The alert number during the session.

6.5.2 Automatic Updates

It is of the utmost importance that the virus definition databases are up-to-date. The product updates them automatically.

Information about the latest virus definition database update can be found at: http://www.F-Secure.com/download-purchase/updates.shtml

Updates enabled — Enable and disable the automatic virus definition updates. By default they are enabled.

Policy Manager Proxies

Displays a list of virus definition database update sources and F-Secure Policy Manager proxies.

If no update servers are configured, the product retrieves the latest virus definition updates from F-Secure Update Server automatically.

PM Proxy address — Displays the URL of the update source.

Priority	Displays the priority level of the update source. The priority numbers are used to define the order in which the host tries to connect servers. Virus definition updates are downloaded from the primary sources first, secondary update sources can be used as a backup. The product connects to the source with the smallest priority number first (1). If the connection to that source fails, it tries to connect to the source with the next smallest number (2) until the connection succeeds. To add a new address to the list, enter the url to the *Address* field and define the priority level of the new address. Click **Add PM Proxy** to add the new entry to the list.
HTTP Proxy	
Use HTTP Proxy	Use an HTTP proxy server to download database updates.
HTTP Proxy Address	Enter the HTTP proxy server address.
Periodic updates	
Automatic updates interval	Define (in minutes) how often the product checks the virus definition database update sources for new updates.
Intermediate server failover time	Define (in minutes) the failover time to connect to specified update servers. If the product cannot connect to update servers during the specified time, it retrieves the latest virus definition updates from F-Secure Update Server if *Allow fetching updates from F-Secure Update Server* is enabled.

Allow fetching updates from F-Secure Update Server	Enable the product to download virus definition updates from F-Secure Update Server when it cannot connect to specified update servers.
Launch scan after updates	Select whether a virus scan should be launched automatically after the virus definitions have been updated. The virus scan scans all local files and directories and it can take a long time. The scan uses the manual scanning settings. By default, the scan is not launched automatically.
Reminders	
Send reminders	If the virus definition databases have not been updated in a while, the product can be set to send a reminder. To enable reminders, check the *Send reminders* check box and set the database age in days when reminders are sent.
Database age in days before reminders are sent	Specify the age of the virus definition databases when they are considered old (3-30 days, the default value is 7 days). An alert is sent as a reminder when the database is older than the specified age.

Using F-Secure Anti-Virus Proxies

F-Secure Anti-Virus Proxy offers a solution to bandwidth problems in distributed installations of F-Secure Anti-Virus Linux Server Security by significantly reducing load on networks with slow connections. When you use F-Secure Anti-Virus Proxy as an updates source, F-Secure products can be configured to retrieve virus definition database updates from a local update repository rather than from the central F-Secure Policy Manager Server.

For information about how to install and configure F-Secure Anti-Virus Proxy, see chapter F-Secure Anti-Virus Proxy in F-Secure Policy Manager Administrator's Guide.

6.5.3 About

The About page displays the license terms, the product version number and the database version.

If you are using the evaluation version of the product, you can enter the keycode in the About page to upgrade the product to the fully licensed version.

7 Command Line Tools

Overview 71
Virus Protection 71
Firewall Protection 72
Integrity Checking 73
General Command Line Tools 74

7.1 Overview

For more information on command line options, see “*Man Pages*”, *96*.

7.2 Virus Protection

You can use the `fsav` command line tool to scan files and the `dbupdate` command line tool to update virus definition databases from the shell.

7.2.1 fsav

Follow these instructions to scan files from the shell:

- To scan all default file types on all local disks, type:

  ```
  fsav /
  ```

- To scan all files in a directory and its subdirectories, enter the directory name. For example:

  ```
  fsav mydirectory
  ```

- To scan a single file, enter the file name (without wildcards). For example:

  ```
  fsav myfile.exe
  ```

Note that the recursive scan detects mounted network file system subdirectories and does not scan network file systems. Scanning a network file system from the client workstation would create unnecessary load on the network and it is much slower than scanning the local file system.

If you want to scan the network file system, run `fsav /` on the server.

If you cannot run `fsav` on the server, you can scan the network file system from the client workstation by explicitly specifying mounted network file system directories on the `fsav` command line.

For example, if an NFS file system is mounted in /mnt/server1, scan it with the following command:

```
fsav /mnt/server1
```

For more information on command line options, see the `fsav` man pages or type `fsav --help`.

7.2.2 dbupdate

Before you can update virus definition databases manually, you have to disable the periodic database update. To disable periodic database updates, edit the crontab of root:

1. Run the following command

   `crontab -e`
2. Add # to the beginning of the following line to comment it out:

   `*/1 * * * * /opt/f-secure/fsav/bin/fsavpmd --dbupdate-only >/dev/null 2>&1`

Follow these instructions to update virus definition databases manually from the command line:

1. Download the fsdbupdate.run file from:

   http://download.f-secure.com/latest/fsdbupdate.run

   fsdbupdate.run is a self-extracting file that stops the automatic update agent daemon, updates databases and restarts the automatic update agent.
2. Run `fsdbupdate.run` as root user.
3. Run `dbupdate` as root user.

7.3 Firewall Protection

You can use the `fsfwc` command line tool to view and change the current security profile.

7.3.1 fsfwc

Use the following command to change the current security profile:

```
/opt/f-secure/fsav/bin/fsfwc --mode {block, mobile, home,
office, strict, normal, bypass}
```

For more information about security profiles, see "*Security Profiles*", *50*.

7.4 Integrity Checking

You can use the `fsic` command line tool to check the system integrity and `fsims` to use the Software Installation Mode from the shell.

7.4.1 fsic

You can create the baseline, add files to the baseline and verify the baseline with the `fsic` command line tool.

Creating the Baseline

Follow these instructions to create the baseline from the command line:

1. Run the fsic tool with the --baseline option:

   ```
   fsic --baseline
   ```

2. Select the files to add to the baseline. If you want to add all files in the directory in the Known Files List in the baseline, type A in the prompt.
3. Enter a passphrase to create the signature.

Adding Files to the Baseline

Follow these instructions to add files to the baseline from the command line. In this example, the product is also configured to send an alert about unauthorized modification attempts of the protected files.

1. Run the *fsic* tool with the --add, --alert and --protect options:

   ```
   /opt/f-secure/fsav/bin/fsic --add --alert=yes
   --protect=yes /etc/passwd /etc/shadow
   ```

2. Recalculate the baseline. The baseline update progress is displayed during the process, and you are prompted to select whether to include the new files in the baseline:

   ```
   /opt/f-secure/fsav/bin/fsic --baseline
   ```

3. Enter a passphrase to create the signature.

Verifying the Baseline

Follow these instructions to verify the baseline from the command line:

1. Run the command:

   ```
   /opt/f-secure/fsav/bin/fsic
   ```

2. Enter the passphrase that you used when you created the baseline.
3. The product validates files and displays whether the files are intact.

7.4.2 fsims

Use the following command to enable Software Installation Mode:

```
/opt/f-secure/fsav/bin/fsims on
```

After you have installed the new software, disable the Software Installation Mode to restore the normal protection level:

```
/opt/f-secure/fsav/bin/fsims off
```

For more information about the Software Installation Mode, see “*Software Installation Mode*”, *60*.

7.5 General Command Line Tools

You can use the `fssetlanguage` command line tool to set the language used in the web user interface.

7.5.1 fssetlanguage

Use the following command to set the language:

```
/opt/f-secure/fsav/bin/fssetlanguage <language>
```

Where language is:

en - english

ja - japanese

de - german

7.5.2 fsma

Use the following command to check the status of the product modules:

```
/etc/init.d/fsma status
```

The following table lists all product modules:

Module	Process	Description
F-Secure Alert Database Handler Daemon	/opt/f-secure/fsav/sbin/fsadhd	Stores alerts to a local database. Alerts can be viewed with the web user interface.
F-Secure FSAV Policy Manager Daemon	/opt/f-secure/fsav/bin/fsavpmd	Handles all F-Secure Policy Manager Console operations (for example, *Scan all hard disks now*, *Update database now*, *Reset statistics*)
F-Secure Firewall Daemon	/opt/f-secure/fsav/bin/ fsfwd.run	The interface between F-Secure Management Agent and the iptables/netfilter firewall.
F-Secure FSAV License Alerter	/opt/f-secure/fsav/libexec/ fslmalerter	Checks and informs how many days are left in the evaluation period when the product is installed in the evaluation mode.
F-Secure FSAV On-Access Scanner Daemon	/opt/f-secure/fsav/sbin/fsoasd	Provides all real-time protection features: real-time virus scanning, real-time integrity checking and rootkit protection.

Module	Process	Description
F-Secure FSAV Status Daemon	/opt/f-secure/fsav/bin/fstatusd	Checks the current status of every component keeps desktop panel applications and web user interface up-to-date.
F-Secure FSAV Web UI	/opt/f-secure/fsav/tomcat/bin/catalina.sh start	Handles the web user interface.
F-Secure FSAV PostgreSQL daemon	/opt/f-secure/common/postgresql/bin/startup.sh	Stores alerts that can be viewed with the web user interface.

7.5.3 fsav-config

If you install the product using RPM packages, you have to use the following command to fsav-config command line tool to create the initial product configuration:

/opt/f-secure/fsav/fsav-config

A Installation Prerequisites

All 64-bit Distributions 78
Red Hat Enterprise Linux 4 78
Debian 3.1 and Ubuntu 5.04, 5.10, 6.06 79
SuSE 80
Turbolinux 10 80

A.1 All 64-bit Distributions

Some 64-bit distributions do not install 32-bit compatibility libraries by default. Make sure that these libraries are installed. The name of the compatibility library package may vary, see the documentation of the ditribution you use for the package name for 32-bit compatibility libraries.

On 64-bit Ubuntu, install *ia32-libs*.

A.2 Red Hat Enterprise Linux 4

Follow these instructions to install the product on a server running Red Hat Enterprise Linux 4 AS:

1. Install the following RPM packages from RHEL4 CDs.
   - Use the command `rpm -ivh <rpm files>`,
   - Use *Applications* > *System Settings* > *Add/Remove Applications*, or
   - Use `up2date`.

   Make sure you have all the following RPM packages installed:
   - gcc
   - glibc-devel
   - glibc-headers
   - glibc-kernheaders

   Make sure you have at least one of the following RPM packages installed:
   - kernel-devel
   - kernel-hugemem-devel
   - kernel-smp-devel

   Use the `uname -r` command to see the current kernel version information.

The system tray applet requires the following RPM packages:

- kdelibs
- compat-libstdc++

2. Install the product normally.

A.3 Debian 3.1 and Ubuntu 5.04, 5.10, 6.06

To install the product on a server running either Debian 3.1 or Ubuntu 5.04, 5.10 or 6.06:

1. Install a compiler, kernel headers and RPM before you install the product.

   Debian:

   ```
   sudo apt-get install gcc rpm make libc6-dev
   sudo apt-get install kernel-headers-`uname -r | cut -d- -f 1-`
   ```

   Ubuntu:

   ```
   sudo apt-get install gcc rpm make libc6-dev
   sudo apt-get install linux-headers-`uname -r`
   ```

2. If you are using Ubuntu 5.10, make sure that *gcc-3.4* package is installed.
3. If you want to use the system tray applet, run the following commands:

   Debian:

   ```
   sudo apt-get install kde-core
   ```

   Ubuntu:

   ```
   sudo apt-get install kdelibs libstdc++5
   ```

4. If you want to enable logins to the Web User Interface, comment (add a hash sign (#) at the beginning of the line) the following line in */etc/pam.d/login*:

   ```
   auth     requisite     pam_securetty.so
   ```

5. Install the product normally.

A.4 SuSE

To install the product on a server running SuSE version 9.1, 9.2, 9.3 or 10.0:

1. Before you install the product, make sure that *kernel-source*, *make* and *gcc* packages are installed. Use YaST or another setup tool.
2. Install the product normally.

A.5 Turbolinux 10

Turbolinux kernel sources may not be configured and so they cannot be used to compile kernel drivers. To fix this, run the following command in the kernel source tree:

```
make oldconfig
```

B Installing Required Kernel Modules Manually

Introduction 82
Before Installing Required Kernel Modules 82
Installation Instructions 82

B.1 Introduction

This section describes how to install required kernel modules manually. You may need to do this in the following cases:

- You forgot to use Software Installation Mode and the system is not working properly.
- In large installations some hosts may not include development tools or kernel source.

B.2 Before Installing Required Kernel Modules

Before installing required kernel modules, you must do the following:

- Make sure that the running kernel version is the same as the version of the kernel sources installed. The kernel configuration must also be the same.
- On some distributions, such as older SUSE distributions, you may need to go to */usr/src/linux* and run commands `make cloneconfig` and `make modules_prepare` before the kernel sources match the installed kernel.

B.3 Installation Instructions

Follow the instructions below to install required kernel modules:

1. Run the following command as the root user:

   ```
   /opt/f-secure/fsav/bin/fsav-compile-drivers
   ```

2. If the summary page in the user interface does not show any errors, the product is working correctly.

`fsav-compile-drivers` is a shell script that configures and compiles the Dazuko driver automatically for your system and for the product. For more information on the Dazuko driver, visit www.dazuko.org.

You can download the Dazuko driver from www.dazuko.org and use it with the product, but it is not recommended. The product has been extensively tested only with the Dazuko version that ships with the product, which is installed in */opt/f-secure/fsav/dazuko.tar.gz*.

If your Linux distribution has a preinstalled Dazuko, it cannot be used as Dazuko depends on the included patches and configuration options, which are likely different in the preinstalled Dazuko. Uninstall the preinstalled Dazuko or make sure that it is not run during the system startup and follow the installation instructions above to install Dazuko with all required patches and configuration options.

C List of Used System Resources

Overview 85
Installed Files 85
Network Resources 85
Memory 86
CPU 86

C.1 Overview

This appendix summarizes the system resources used by the product.

C.2 Installed Files

All files installed by the product are in the following directories:

/opt/f-secure

/etc/opt/f-secure

/var/opt/f-secure

In addition, the installation creates the following symlinks:

/usr/bin/fsav -> /opt/f-secure/fssp/bin/fsav

/usr/bin/fsic -> /opt/f-secure/fsav/bin/fsic

/usr/bin/fsui -> /opt/f-secure/fsav/bin/fsui

/usr/share/man/man1/fsav.1 -> /opt/f-secure/fssp/man/fsav.1

/usr/share/man/man8/fsavd.8 -> /opt/f-secure/fssp/man/fsavd.8

C.3 Network Resources

When running, the product reserves the following IP ports:

Interface	Protocol	Port	Comment
lo	tcp	28005	Web User Interface internal communication port
lo	tcp	28078	PostgreSQL alert database
lo	tcp	28080	Local Web User Interface access
any	tcp	28082	Remote SSL Web User Interface access (if enabled)

C.4 Memory

The Web User Interface reserves over 200 MB of memory, but since the WebUI is not used all the time, the memory is usually swapped out. The other product components sum up to about 50 MB of memory, the on-access scanner uses the majority of it.

The memory consumption depends on the amount of file accesses on the system. If several users are logged in to the system and all of them access lots of files, the memory consumption grows.

C.5 CPU

The load on the processor depends on the amount of file accesses on the system, as the on-access scanner scans every file that is opened and closed.

The CPU usage grows when many users are logged in to the system at the same time.

Some software products are designed to access many files and the on-access scanning can slow down these products noticeably.

D Troubleshooting

User Interface 88
F-Secure Policy Manager 89
Integrity Checking 89
Firewall 91
Virus Protection 93
Generic Issues 93

D.1 User Interface

Q. I cannot log in to the Web User Interface. What can I do?

A. On some distributions, you have to comment (add a hash sign (#) at the beginning of the line) the following line in */etc/pam.d/login*:

```
# auth     requisite     pam_securetty.so
```

Q. The F-icon in the system tray has a red cross over it, what does it mean?

A. When the F-icon has a red cross over it, the product has encoutered an error. Open the Web User Interface to see a detailed report about the issue.

To fix the problem, try to restart the product. Run the following command:

```
/etc/init.d/fsma restart
```

Q. How can I get the F-icon visible in the systray?

A. You may need to logout and login again to get the F-icon in your systray. If you are using Gnome Desktop, make sure you have a notification area in your Gnome Panel.

Q. How do I enable the debug log for the web user interface?

A. Change */opt/f-secure/fsav/tomcat/bin/catalina.sh* from:

```
#CATALINA_OUT="$LOGS_BASE"/catalina.out
CATALINA_OUT=/dev/null
```

to:

```
CATALINA_OUT="$LOGS_BASE"/catalina.out
#CATALINA_OUT=/dev/null
```

The logfile is in */var/opt/f-secure/fsav/tomcat/catalina.out*.

D.2 F-Secure Policy Manager

Q. How can I use F-Secure Linux Server Security with F-Secure Policy Manager 6.0x for Linux?

A. F-Secure Policy Manager Server has to be configured to retrieve new riskware and spyware databases for the product.

Note that these instructions apply to F-Secure Policy Manager Server 6.0x for Linux only, the product is not compatible with other Linux or Windows F-Secure Policy Manager Server versions.

Add a line to the */etc/opt/f-secure/fspms/fspms-fsauasc.conf* file by running this command:

```
echo "avpe=republish" >> /etc/opt/f-secure/fspms/
fspms-fsauasc.conf
```

D.3 Integrity Checking

Q. Symlinks are not working for Integrity Checking or Rootkit Protection, what can I do?

A. You may be denied to load a kernel module if the file containing the kernel module is a symlink and the real file where the symlink points to is not in the Integrity Checking baseline. The same applies if *modprobe* or *insmod* utilities (the module loaders) use files or libraries which are symlinks and the file where the symlink points to is not in the baseline.

For example, modprobe uses */lib/libz.so.1*, which is really a symlink to a real file */lib/libz.so.1.2.2*. The symlink is in the baseline but the real file is not. In this case, *modprobe* is not allowed to run as it tried to open a file that is not in the baseline.

You should never add only symlinks to the baseline, you should always add both the symlink and the real file where the symlink points.

Q. I forgot to use Software Installation Mode and my system is not working properly. What can I do?

A. Create a new baseline. Execute the following commands:

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -
fsic --baseline
```

Q. Can I update the Linux kernel when I use Integrity Checking?

A. Use the Software Installation Mode. After you have updated the kernel, disable the Software Installation Mode to restore the normal protection level. For more information, see “*Software Installation Mode*”, *60*.

Q. There are too many modified files to update with the user interface.

A. Create a new baseline. Execute the following commands:

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -
fsic --baseline
```

Q. The Integrity Checking page in the user interface does not display all entries. How can I fix this?

A. If you have many (over 10000) files in the baseline, you may have to adjust the memory settings of the Java Virtual Machine view all entries in the baseline.

a. Edit */opt/f-secure/fsav/tomcat/bin/catalina.sh* file:

Replace

```
JAVA_OPTS=-Djava.library.path=/opt/f-secure/fsav/
tomcat/shaj
```

with

```
JAVA_OPTS="-Djava.library.path=/opt/f-secure/fsav/
tomcat/shaj -Xmx256M"
```

b. Restart the product to take new settings into use:

```
/etc/init.d/fsma restart
```

Q. Do I have to use the same passphrase every time I generate the baseline?

A. No, you have to verify the baseline using the same passphrase that was used when the baseline was generated, but you do not have to use the same passphrase again when you generate the baseline again.

D.4 Firewall

Q. After installing the product, users cannot access samba shares on my computer, how can I fix this?

A. The *Office* firewall profile contains a rule that allows Windows Networking but that rule is disabled by default. Enable the rule to allow accesses to samba shares.

Q. After intalling the product, I cannot browse local are network domains and workgroups (SMB). How can I fix this?

A. You need to add a rule to the firewall that allows browsing Windows shares on your local area network. Follow these instructions:

a. Go to *Firewall* > *Network Services* page in the Web User Interface advanced mode.
b. Click **Add new service**.
c. Create the following service:

```
Service Name: Windows Networking Local Browsing
Protocol: UDP
Initiator ports: 137-138
Responder: >1023
Description SMB LAN browsing
```

d. Click **Add as a new service** and **Save**.
e. Go to the firewall menu and click **Firewall Rules**.
f. Click **Add new rule**.
g. Create the following rule:

```
Type: ACCEPT
Remote Host: [myNetwork]
Description: Windows Networking Local Browsing
Service (select box): Windows Networking Local
Browsing
Direction: in
```

h. Click **Add Service to this Rule** and **Add to Firewall Rules**. The new rule should be visible at the bottom of the firewall rule list. If you cannot see the rule, click **>>** to move to the end of the list.

i. Click on the up arrow next to the new ruleto move the rule above any "Deny rest" rule.

j. Click **Save** to save your new rule set and apply new firewall rules. Your SMB LAN browsing should work now.

Q. How can I set up firewall rules to access NFS servers?

A. You need to allow the following network traffic through the firewall:

- portmapper (tcp and udp port 111)
- nfsd (tcp and udp 2049)
- mountd (variable port from portmapper)

Mountd is needed only when the NFS share is mounted. After the mount is completed, all traffic is to the nfsd.

As the mountd port is not always the same, follow these instructions to mount NFS shares:

- Either turn off the firewall, mount (or umount) the NFS share and turn on the firewall again, or
- on the NFS server, start mountd with the --port PORT option, which forces mountd to use a fixed port number instead of a random port. Then, create a firewall rule that allows udp and tcp traffic to that port number.

D.5 Virus Protection

Q. How do I enable the debug log for real-time virus scanner?

A. In Policy Manager Console, go to *Product/Settings/Advanced/* and set *fsoasd log level* to *Debug*.

In standalone installation, run the following command:

```
/opt/f-secure/fsma/bin/chtest s 44.1.100.11 9
```

The above command works for Client Security product. If you are using Server Security, replace 44 with 45.

The log file is in */var/opt/f-secure/fsav/fsoasd.log*

Q. How can I use an HTTP proxy server to downloading database updates?

A. In Policy Manager Console, go to *F-Secure Automatic Update Agent* / *Settings* / *Communications* / *HTTP Settings* / *User-defined proxy settings* and set *Address* to:

```
http://[[user][:pass]@]proxyhost[:port]
```

In Web User Interface, use the setting in the Automatic Updates page in the advanced mode.

Q. Does the real-time scan work on NFS server?

A. If the product is installed on NFS server, the real-time scan does not scan files automatically when a client accesses a file on the server.

D.6 Generic Issues

Q. How can I clean an interrupted installation?

A. If the product installation is interrupted, you may have to remove the product components manually.

a. List all installed rpm packages:

```
rpm -qa | grep f-secure
rpm -qa | grep fsav
```

b. Remove installed packages. Run the following command for each installed package:

```
rpm -e --noscripts <package_name>
```

c. 3. Remove all of the product installation directories:

```
rm -rf /var/opt/f-secure/fsav
rm -rf /var/opt/f-secure/fsma
rm -rf /etc/opt/f-secure/fsav
rm -rf /etc/opt/f-secure/fsma
rm -rf /opt/f-secure/fsav
rm -rf /opt/f-secure/fsma
```

Q. System is very slow. What is causing this?

A. The real-time virus scan and Integrity Checking can slow down the system.

- Use the basic Linux tools (`top` and `vmstat`) to check what is slowing down the system.
- Make sure that you are using the dazuko version that is shipped with the product.
- If a file that is accessed often is time-consuming to scan, consider adding it to the excluded list. For more information, see "*Real-Time Scanning*", *40*.
- If you are using the centralized administration mode, make sure that the DNS queries return addresses quickly or use IP addresses with F-Secure Policy Manager.

Q. The product is unable to contact the database, how can I fix this?

A. Sometimes, after a hard reset for example, the product may be unable to contact the database. Follow these instructions to resolve the issue:

a. As root, remove the database PID file:

```
rm /var/opt/f-secure/fsav/pgsql/data/postmaster.pid
```

b. As root, restart the product:

```
/etc/init.d/fsma restart
```

Q. I get reports that "F-Secure Status Daemon is not running", how can I start it?

A. Sometimes, after a hard reset for example, F-Secure Status Daemon may fail to start. Restart the product to solve the issue:

```
/etc/init.d/fsma restart
```

Alternatively, you may start F-Secure Status Deamon manually:

```
/opt/f-secure/fsav/bin/fstatusd
```

Q. I need to compile kernel drivers manually, how do I do that?

A. You may need to compile kernel drivers that the product need manually, if

- you did not have compilers and other required tools intalled during the installation,
- you did not have kernel headers or sources installed during the installation, or
- you have upgraded the kernel and you need to compile drivers for the new kernel.

To compile and install drivers, run the following command:

```
/opt/f-secure/fsav/bin/fsav-compile-drivers
```

E Man Pages

fsav 97
fsavd 131
dbupdate 149
fsfwc 153
fsic 156

fsav

command line interface for *F-Secure Anti-Virus*

`fsav` *options target ...*

Description

`fsav` is a program that scans files for viruses and other malicious code. `fsav` scans specified targets (files or directories) and reports any maliciouscode it detects. Optionally, `fsav` disinfects, renames or deletes infected files.

The types of viruses *F-Secure Anti-Virus* detects anddisinfects include but are not limited to: Linux viruses, macro viruses infecting Microsoft Office files, Windows viruses and DOS file viruses. *F-Secure Anti-Virus* can also detect spyware, adware and other riskware (in selected products). `fsav` can scan files inside ZIP, ARJ, LHA, RAR, GZIP, TAR, CAB and BZ2 archives and MIME messages. *F-Secure Anti-Virus* utilizes three scanners to scan files: *F-Secure Corporation Orion and Libra scan engines* and *Kaspersky Lab AVP scan engine*.

`fsav` requires the `fsavd` scanner deamon to scan files. fsav uses UNIX domain sockets to communicate with the daemon. If fsavd is not running, `fsav` launches fsavd before the scan.

Options

`--action1={none|report,disinf|clean,rename,delete|remove,abort,custom|exec}`

Synonym to `--virus-action1`, deprecated.

`--action2={none|report,disinf|clean,rename,delete|remove,abort,custom|exec}`
Synonym to `--virus-action2`, deprecated.

`--action1-exec=PROGRAM` *F-Secure Anti-Virus* runs PROGRAM if the primary action is set to custom/exec.

`--action2-exec=PROGRAM` *F-Secure Anti-Virus* runs PROGRAM if the secondary action is set to custom/exec.

`--action-timeout={e,c}` What to do when the scan times out: Treat the timeout as error (e) or clean (c).

`--archive[={on,off,yes,no,1,0}]` Scan files inside archives (default). Archives are still scanned as normal files with or without this option. See NOTES -section below about nested archives.

`--auto[={on,off,yes,no,1,0}]` Disable action confirmation. Assumes 'Yes' to all enabled actions.

`--avp[={on,off,yes,no,1,0}]` Enable/disable the AVP scanning engine for the scan and the disinfection. If any engine is enabled, all other engines are disabled (unless

explicitly enabled).

`--config={file[:PATH]|fsma[:OID]}` `file`: Use the configuration file based management method optionally using PATH as the configuration file instead of the default configuration file (`/etc/opt/f-secure/fssp/fssp.conf`).

`fsma`: Use the F-Secure Policy Manager based management method optionally specifying the OID used in sending alerts.

`--databasedirectory=`*`path`* Read virus definition databases from the directory *`path`*. The default is `"."`.

This option cannot be used to change the database directory of fsavd that is running. The option is effective only when fsav launches fsavd.

The default value is `/var/opt/f-secure/fsav/databases/`.

`--dbupdate=`*`update directory`* Initiate the database update from the update directory. The update directory should contain new virus definition databases.

Warning

Do not use this option directly from the

command-line! This option is intended to be used only with the `dbupdate` script.

`--allfiles[={on,off,yes,no,1,0}]` Scan all files regardless of the extension. By default, the setting is on. (In previous versions, this option was called 'dumb'.)

`--exclude=`*`path`* Do not scan the given path.

`--exclude-from=`*`file`* Do not scan paths listed in the file. Paths should be absolute paths ending with a newline character.

`--extensions=`*`ext,ext,...`* Specify the list of filename extensions to be scanned. You can use “?” or “*” as wildcard characters.

The default list is:

*

`--help` Show the short help of command line options and exit.

`--input` Read files to scan from the standard input.

`--libra[={on,off,yes,no,1,0}]` Enable/disable the Libra scanning engine for the scan and the disinfection. If any engine is enabled, all other engines are disabled unless explicitly enabled.

`--list[={on,off,yes,no,1,0}]` List all files that are scanned.

`--maxnested=`*`value`* Should be used together with the `--archive` option. Set the maximum number of nested archives (an archive containing another archive). If the fsav encounters an archive that contains more nested archives than the specified value, it reports a scan error for the file. See NOTES -section below about nested archives.

If the value is set to 0, the archive is scanned but if it contains another archive, fsav reports a scan error for the file.

The default value is 5.

`--mime[={on,off,yes,no,1,0}]` Enable MIME message scanning. MIME messages are scanned the same way as archives and the --maxnested option applies to them as well.

`--noinvalidmime` Ignore MIME header anomalies.

`--nomimeerr` Ignore MIME decoding errors.

`--nomimepart` Ignore errors due to partial MIME content.

`--nopass` Ignore password-protected archives.

NOTE: Certain password- protected archives are reported as suspected infections instead of password-protected archives.

`--orion[={on,off,yes,no,1,0}]` Enable/disable the Orion scanning engine for the scan and the disinfection. If any engine is enabled, all other engines are disabled unless explicitly enabled.

`--preserveatime[={on,off,yes,no,1,0}]` Preserve the last access time of the file after it is scanned. If the option is enabled, the last access time of the file does not change when it is scanned. The option can be used for example with some back-up systems that back up only files that have an updated last access time field.

`--raw[={on,off,yes,no,1,0}]` Write ESC character (\033) as is to output. By default ESC character is shown in reverse video as string “<ESC>”.

`--riskware[={on,off,yes,no,1,0}]` Report riskware detections. Riskware is potential spyware. This feature is available in selected products.

`--riskware-action1={none|report,rename,delete|remove}` Primary action to take when riskware is found: report only (to terminal and as an alert), rename, or delete/

remove.

`--riskware-action2={none|report,rename,delete|remove}` Secondary action to take if primary action fails. Parameters are the same as for primary action.

`--scanexecutables[={on,off,yes,no,1,0}]` Enable the executable scanning. If a file has any of user/group/other executable bits set, it is scanned regardless of the file extension.

`--scantimeout=`*value* Set a time limit in seconds for a single file scan or disinfection task. If scanning or disinfecting the file takes longer than the specified value, fsav reports a scan error for the file.

If the value is set to 0 (default), the scan timeout is disabled and the file is scanned until the scan finishes (or a scan error occurs).

`--short[={on,off,yes,no,1,0}]` Use the short output format. Only the path to infected or renamed files is shown.

`--shutdown` By default, fsavd does not immediately exit after completing a file scan but hangs around waiting for new scan tasks. This option can be used to make an idle fsavd exit immediately.

`--silent[={on,off,yes,no,1,0}]` Do not generate any output (except error messages).

`--socketname=`*`socket path`* Use the given socket path to communicate with fsavd. The default socket path is `/tmp/.fsav-<UID>`, or `/tmp/.fsav-<UID>-sa`, if fsav is started with the `--standalone` option.

`--status` Show the status of the fsavd scanning daemon and exit. If the daemon is running, the exit code is zero. Otherwise, the exit code is non-zero.

NOTE: Usually, a scanning daemon which is not running is not an error, as fsav launches the daemon before the scan by default. The daemon that was launched by fsav exits after some idle time. To run a permanent instance of the scanning daemon, see fsavd(8).

`--suspected-action1={none|report,rename,delete|remove}` Primary action to take when a suspected virus infection is found: report only (to terminal and as an alert), rename, or delete/remove.

`--suspected-action2={none|report,rename,delete|remove}` Secondary action to take if the primary action fails. Parameters are the same as for primary action.

`--standalone[={on,off,yes,no,1,0}]` Use the

standalone version to scan files. The option forces the launch of a new fsavd.

`--stoponfirst[={on,off,yes,no,1,0}]` Stop after finding the first infection with any scan engine. If file contains multiple infections, only the first is reported. If several scan engines can detect the infection, only the first one is reported. By default, the option is disabled.

`--symlink[={on,off,yes,no,1,0}]` Follow symbolic links. Symbolic links are not followed by default.

`--usedaemon[={on,off,yes,no,1,0}]` Use the existing daemon to scan files. fsavd must be running or the command fails. See fsavd(8) for more information.

If the connection to the server fails, fsav generates an error. Without this option, if the connection fails, fsav launches fsavd automatically.

`--skiplarge[={on,off,yes,no,1,0}]` Do not scan files equal or larger than 2 GB (2,147,483,648 bytes). If this option is not set, an error will be reported for large files.

`--version` Show *F-Secure Anti-Virus* version, engine versions and dates of database files, and exit.

Note

Database versions contain date of the databases only. There may be several databases released on same day. If you need more detailed version information, open `header.ini` in the database directory and search for the following lines:

```
[FSAV_Database_Version]
Version=2003-02-27_03
```

The string after “Version=” is the version of databases.

`--virus-action1={report,disinf|clean,rename,delete|remove,abort, custom|exec}` Primary action to take when a virus infection is found: report only (to terminal and as an alert), disinfect/clean, rename, delete/remove, abort scanning or execute a user-defined program (custom/exec).

`--virus-action2={report,disinf|clean,rename,delete|remove,abort, custom|exec}` Secondary action to take if primary action fails. Parameters are the same as for primary action.

SCAN REPORTS

By default, fsav reports the infected and suspected infections to stdout. Scan errors are reported to stderr.

An example of an infection in the scan report:

```
                /tmp/eicar.com:      Infected:
    EICAR-Test-File [AVP]
```

where the file path is on the left, the name of the infection in the middle and the name of the scan engine that reports the infection in brackets.

An example of a suspected infection in the scan report:

```
       /tmp/sample.img:  Suspected:  Type_Boot
    [AVP]
```

which differs from infected output only by the type of the suspection in the middle.

The following suspections can occur when the MIME scanning is enabled:

Partial MIME message.

Explanation: Partial MIME messages are splitted into several files and cannot be scanned. Typically, the message contains the following header information 'Content-Type: message/partial;'.

MIME decompression error.

Explanation: Scanned MIME message uses non-standard

encoding and cannot be scanned.

`Invalid MIME header found.`

Explanation: Scanned MIME message uses non-standard header and cannot be scanned.

The `--list` option shows the clean files in the report. An example of the output:

```
/tmp/test.txt - clean
```

The `--archive` option scans the archive content and the output is as follows for the infected or suspected archive content:

```
[/tmp/eicar.zip] eicar.com: Infected:
EICAR-Test-File [AVP]
```

where the path to the archive surrounded by brackets is on the left followed by the path to the infected file in the archive. In the current release, the nested archives and the clean archive content is not listed in the output.

ACTIONS

fsav can be instructed to take actions on infected files. Possible actions are: report, disinfect/clean, rename, delete/remove, abort or custom/exec. There is a primary action, which is taken first. If the primary action fails a secondary action is executed.

The default primary action is disinfect and the default second-

ary action is rename.

fsav must have write access to the file to be disinfected. Disinfection is not always possible and fsav may fail to disinfect a file. Especially, files inside archives cannot be disinfected.

Infected files are renamed to `<original_filename>.virus` and clears executable and SUID bits from the file. Suspected files are renamed to `<original_filename>.suspected`. Riskware files are renamed to `<original_filename>.riskware`. The user running the scan must have write access to the directory in order to rename the file.

The delete action removes the infected/suspected/riskware file. The user running the scan must have write access to the directory in order to delete the file.

By default, actions are confirmed before the execution. For example, for the disinfection fsav asks the following confirmation:

```
   eicar.com: Disinfect? (Yes, No, yes to
All)
```

where the answer 'Y', 'y', 'Yes' or 'yes' confirms the action.

The answer 'A', 'a', 'All' or 'all' automatically confirms any further disinfections. If other actions are enabled, they are still confirmed unless they are automatically confirmed as well.

Any other answer will not confirm the action and the action is not taken. An action not taken is treated the same way as an

action that failed, i.e. if the user does not want to take the primary action, the secondary action is tried next.

The action confirmation can be disabled with `--auto` -option.

WARNINGS

fsav warnings are written to the standard error stream (stderr). Warnings do not stop the program. fsav ignores the reason for the warning and the execution continues as normal.

Unknown option '<*user given option name*>' in configuration file <*file path*> line <*line number*>

Explanation: The configuration file contains an unknown option name.

Resolution: Edit the configuration file.

Configuration file <*file path*> has invalid syntax at line <*line number*>

Explanation: The parsing of the configuration file has failed because of the invalid syntax.

Resolution: Edit the configuration file.

Could not open exclude file <*file path*>: <*OS error*>

Explanation: A file path to the `exclude` -option does not exist or is not accessible.

Resolution: Edit command-line options.

Illegal archive scanning value '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `archivescanning` field in the configuration file has an incorrect value.

Resolution: Edit the configuration file and set the archivescanning field to one of the following: 1 or 0. Restart fsav to take new values in use.

Illegal MIME scanning value '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `mimescanning` field in the configuration file has an incorrect value.

Resolution: Edit the configuration file and set the mimescanning field to one of the following: 1 or 0. Restart fsav to take new values in use.

Illegal scan executables value '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `scanexecutables` field in the configuration file has an incorrect value.

Resolution: Edit the configuration file and set the scanexecutables field to one of the following: 1 or 0. Restart fsav to take new values in use.

Maximum nested archives value '<*user given value*>'

is not valid in configuration file <*file path*> line <*line number*>.

Explanation: The `maxnestedarchives` field in the configuration file is not a number.

Resolution: Edit the configuration file.

Maximum nested archives value '<*user given value*>' is out of range in configuration file <*file path*> line <*line number*>

Explanation: The `maxnestedarchives` field in the configuration file is less than zero or more than LONG_MAX.

Resolution: Edit the configuration file.

Maximum scan engine instances value '<*user given value*>' is not valid in configuration file <*file path*> line <*line number*>

Explanation: The `engineinstancemax` field in the configuration file is not a number.

Resolution: Edit the configuration file.

Maximum scan engine instances value '<*user given value*>' is out of range in configuration file <*file path*> line <*line number*>

Explanation: The `engineinstancemax` field in the configuration file is less than zero or more than LONG_MAX.

Resolution: Edit the configuration file.

Scan timeout value '<*user given value*>' is not valid in configuration file <*file path*> line <*line number*>

Explanation: The `scantimeout` field in the configuration file is not a valid number.

Resolution: Edit the configuration file.

Scan timeout value '<*user given value*>' is out of range in configuration file <*file path*> line <*line number*>

Explanation: The `timeout` field in the configuration file is less than zero or more than LONG_MAX.

Resolution: Edit the configuration file.

Scan extensions list is too long in configuration file <*file path*> line <*line number*>, list is truncated.

Explanation: The `extensions` field in the configuration file is more than 4096 bytes long.

Resolution: Edit the configuration file.

Unknown action '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `action` field in the configuration file has an incorrect value.

Edit configuration file and set the action field to one of the following: report, disinfect, clean, rename, delete, remove,

abort, custom or exec. Restart fsav to take new values in use.

Unknown syslog facility '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `syslogfacility` ield in the configuration file has an incorrect value.

Resolution: Edit configuration file and set the syslog- facility field to one of the facility names found in syslog(3) manual page. Restart fsav to take new values in use.

FATAL ERRORS

fsav fatal errors are written to the standard error stream (stderr). In case of fatal error program execution stops immediately with exit code 1.

Fatal erros reported by fsav and the descriptions are listed below:

Error: no files to scan.

Explanation: The user has not given files to scan..

Resolution: fsav exits with fatal error status (exit code 1). The user has to correct the command-line parameters and start the fsav again.

Invalid socket path '<*socket path*>': not a socket.

Explanation: The user has given socket path which already exists but is not a socket from configuration file or from command-line.

Resolution: fsav exits with fatal error status (exit code 1). The user has to correct the command-line parameters or configuration file or remove the file from path and start the fsav again.

Invalid socket path '<*socket path*>': <*OS error*>.

Explanation: The user has given invalid socket path from configuration file or from command-line, either socket does not exist or is not accessible.

Resolution: fsav exits with fatal error status (exit code 1). The user has to correct the command-line parameters or configuration file or remove the file from path and start the fsav again.

Input file '<*file path*>' is invalid: <*OS error*>.

Explanation: The user has given invalid input file path, either file does not exist or is not readable.

Resolution: fsav exits with fatal error status (exit code 1). The user has to correct the command-line parameters and start the fsav again.

Unknown command line option '<*option*>'.

Explanation: The user has given unknown option from the command-line.

Resolution: fsav exits with error status. The user has to correct the command-line parameters and start the fsav again.

Could not open configuration file <*file path*>: <*OS error*>

Explanation: The user has given a file path to the `--configfile` option which either does not exist or is not accessible.

Resolution: The user has to correct command-line options and try again.

Scan engine directory '<*directory path*>' is not valid in configuration file at line <*line number*>: <*OS error message*>

Explanation: The user has specified a scan engine directory path which either does not exist, is not accessible or is too long in the configuration file.

Resolution: The user has to correct the path and start fsav again.

Scan engine directory '<*directory path*>' is not valid: <*OS error message*>

Explanation: The user has entered a scan engine directory path which either does not exist, is not accessible or is too long from the command-line.

Resolution: The user has to correct the path and start fsav again.

Database directory '<*directory path*>' is not valid in configuration file at line <*line number*>: <*OS error message*>

Explanation: The user has entered a database directory path which either does not exist, is not accessible or is too long

from the configuration file.

Resolution: The user has to correct the path and start fsav again.

Database directory '<*directory path*>' is not valid: <*OS error message*>

Explanation: The user has entered a database directory path which either does not exist, is not accessible or is too long from the command-line.

Resolution: The user has to correct the path and start fsav again.

Database update directory '<*directory path*>' is not valid in configuration file at line <*line number*>: <*OS error message*>

Explanation: The user has entered a database update directory path which either does not exist, is not accessible or is too long from the configuration file.

Resolution: The user has to correct the path and start fsav again.

Could not open input file <*file path*>: <*OS error*>

Explanation: The user has given a file path to the `input` option which either does not exist or is not accessible.

Resolution: The user has to correct command-line options and try again.

Illegal command line option value '<*user given*>

***option*>'.**

Explanation: The user has entered an unknown command-line option from the command-line.

Resolution: The user has to correct command-line options and try again.

Illegal scan timeout value '<*value*>'.

Explanation: The user has entered an illegal scan timeout value from the command-line.

Resolution: The user has to correct command-line options and try again.

Illegal maximum nested archives value '<*value*>'.

Explanation: The user has entered an illegal maximum nested archives value from the command-line.

Resolution: The user has to correct command-line options and try again.

Given database update path is invalid.

Explanation: The database update path given with `--dbupdate` is invalid, i.e. the path does not exist, it is not accessible or it is not a directory.

Resolution: The user has to correct command-line options and try again.

Server status query failed.

Explanation: The user has tried to request the server version with `version` but the request processing failed.

Resolution: The server is not running. The product may be installed incorrectly. The `installdirectory` is either missing or wrong in the configuration file. The system may be low in resources so launching might have failed because of e.g. insufficient memory.

`Shutdown failed.`

Explanation: The user has tried to request server shutdown with `shutdown` but the request processing failed.

Resolution: If fsavd is not running, the user does not need to do anything. If fsavd is running, but the user does not have rights to access to the socket, the user may try to use kill(1) command to shutdown the server.

`Failed to launch fsavd.`

Explanation: fsavd is not running and fsav has tried to launch fsavd in the stand-alone mode but failed.

Resolution: The product may be installated incorrectly. The `installdirectory` is either missing or wrong in the configuration file. The system may be low in resources so launching might have failed because of e.g. insufficient memory.

Scanning file '<*file path*>' failed: connect to fsavd failed.

Disinfect file '<*file path*>' failed: connect to fsavd failed.

Explanation: The file scanning failed because the connection to fsavd can not be established.

Re-scanning file '<*file path*>' failed due IPC error.

Explanation: The file re-scanning failed because the connection to server is broken.

Resolution: The server has died unexpectly. The user should restart the server and try to scan the file again. If the problem persists, the user should send a bug report and a file sample to F-Secure.

Update directory '<*file path*>' is not valid: <*OS error message*>

Explanation: The database update directory given in the configuration file or from the command-line does not exist or it is not accessible.

Resolution: The user has to change the database update directory and try to update the databases again.

Can not do update from in-use database directory: '<*file path*>'

Explanation: The database update directory given in the configuration file or from the command-line is same as in-use database directory.

Resolution: The user has to change the database update directory and try to update the databases again.

**An other database update in progress, flag file '<*file*

***path*>' exists.**

Explanation: The database directory contains an update flag file which is created while the database update is in progress.

Resolution: The user has to check if an other database update is in progress. If no other update process exists, the user should delete the flag file and try to update the databases again.

Could not create flag file '<*file path*>'.

Explanation: The database directory contains an update flag file which is created while the database update is in progress and the creation of the file has failed.

Resolution: The database update process does not have proper rights to create the flag file and fails. The user has to make sure the update process runs with proper rights or the database directory has proper access rights.

Could not open lock file '<*file path*>'.

Explanation: The database update process has failed to open lock file in the database directory.

Resolution: The database update process does not have proper rights to open the lock file and fails. The user has to make sure the update process runs with proper rights or the database directory has proper access rights.

Could not acquire lock for lock file '<*file path*>'.

Explanation: The database update process has failed to acquire the lock for lock file in the database directory.

Resolution: The database update process does not have proper rights to the lock file and fails. The user has to make sure the update process runs with proper rights or the database directory has proper access rights.

Could not release lock for lock file '<*file path*>'.

Explanation: The database update process has failed to release the lock for the lock file in the database directory.

Resolution: fsavd is halted. The user should stop fsavd and remove the lock file, do database update and start fsavd again.

Database update and restore failed! Server halted.

Explanation: The database update process has failed to perform an update and failed to restore the database backups.

Resolution: fsavd is halted. The user should stop fsavd, remove the update flag file, do database update and start fsavd again.

Database update failed, restored old ones.

Explanation: The database update process has failed to perform the update but succeeded to restore the database backups.

Resolution: The user should try to update the databases again later.

Could not remove update flag file '<*file path*>'. Server halted.

Explanation: The database update process has successfully updated databases, but failed to remove the update flag file.

Resolution: fsavd is halted. The user should remove the update flag file manually.

SCAN ERRORS

fsav scan errors are written to the standard error stream (stderr). In case of scan error file scanning is immediately stopped and the scan continues with next file in input. If no files is found infected or suspected, the scan error is indicated with exit code 9.

Scan erros reported by fsav and the descriptions are listed below:

<file path>*: ERROR: *<OS error message>

Explanation: The file could not be scanned, reason is given in OS error message.

Resolution: Common reason is the file does not exist or is not readable. Check the file path and access rights.

***<file path>*: ERROR: path too long - NOT SCANNED**

Explanation: The file path is too long (> PATH_MAX). The file cannot be scanned.

Resolution: The user has to move the file to a shorter path and try to scan the file again.

***<file path>*: ERROR: Could not open the file**

[<scan engine>]

Explanation: The scan engine could not open the file for scanning because the scan engine does not have a read access to the file.

Resolution: The user has to make file readable for fsavd and try to scan the file again. If the user or fsav launches fsavd, fsavd has same access rights as the user and can only open samexs files the user is authorized to open.

***<file path>*: ERROR: Password protected file [<engine name>]**

Explanation: The scan engine could not open the file for scanning because the file is password protected, i.e. encrypted.

Resolution: The user may try to decrypt the file and try scanning again.

***<file path>*: ERROR: Scan aborted [<scan engine>]**

Explanation: The scanning was aborted for example because of the scan timeout.

Resolution: The user may try scanning the file again.

***<file path>*: ERROR: Scan timeout [<scan engine>]**

Explanation: The scanning was aborted because of the scan timeout.

Resolution: The user may try scanning the file again with bigger scan timeout value.

<*file path*>: ERROR: Could not read from file [<scan engine>]

Explanation: The scanning failed because of read from file failed.

Resolution: The file is probably corrupted and cannot be scanned.

<*file path*>: ERROR: Could not write to file [<scan engine>]

Explanation: The disinfect failed because of write to file failed.

Resolution: The file is write-protected, archive or corrupted and cannot be disinfected.

<*file path*>: ERROR: Internal error: Bad file [<scan engine>]

Explanation: The file scan failed because the scan engine could not handle the file properly.

Resolution: The file is probably corrupted and cannot be scanned.

<*file path*>: ERROR: Maximum nested archives encountered. [<scan engine>]

Explanation: The file scan failed because too many nested archives encountered.

Resolution: Increase maximum nested archives limit and try to scan again.

Scanning file '<*file path*>' failed: connection to fsavd lost due timeout.

Disinfect file '<*file path*>' failed: connection to fsavd lost due timeout.

Explanation: The file scanning failed because the connection to fsavd is lost because of IPC timeout.

Resolution: The server has died unexpectly. The user should restart fsavd and try to scan the file again. If the problem persists, the user should send a bug report and a file sample to F-Secure.

In case of other error messages type of '<filename>: ERROR: <error message> [<scan engine>]' not listed here, the probable source of the error is a problematic file to be scanned. If the same error message appears every time the file is scanned, either exclude the file from the scan or send a sample file to F-Secure Anti-Virus Research. See the instructions for more information.

EXIT CODES

`fsav` has following exit codes:

0	Normal exit; no viruses or suspicious files found.
1	Fatal error; unrecoverable error. (Usually a missing or corrupted file.)

3	A boot virus or file virus found.
4	Riskware (potential spyware) found.
6	At least one virus was removed and no infected files left.
7	Out of memory.
8	Suspicious files found; these are not necessarily infected by a virus.
9	Scan error, at least one file scan failed.
130	Program was terminated by pressing CTRL-C, or by a sigterm or suspend event.

`fsav` reports the exit codes in following priority order:

130, 7, 1, 3, 4, 8, 6, 9, 0.

EXAMPLES

Scan a file 'test.exe' using the default configuration file. If fsavd is not running, fsavd is launched:

```
$ fsav test.exe
```

Scan files in a directory '/mnt/smbshare' which match the extension list:

```
$ fsav --extensions=exe,doc,dot,xls
/mnt/smbshare
```

Scan all files in a directory '/mnt/smbshare':

```
$ fsav /mnt/smbshare
```

Scan all files and archive contents with the scan time limit set to 3 minutes:

```
$ fsav --archive --scantimeout=180
--allfiles /mnt/smbshare
```

Scan and list files with '.EXE' or '.COM' extension in a directory '/mnt/smbshare':

```
$ fsav --list --extensions='exe,com'
/mnt/smbshare
```

Scan and disinfect or rename infected/suspected files without confirmation:

```
$ fsav --virus-action1=disinf
--virus-action2=rename --auto /mnt/smb-
share
```

Scan files found by find(1) -command and feed the scan report to the mail(1) command:

```
$ find /mnt/smbshare -type f | \
  fsav --input 2>&1 | \
  mail -s 'FSAV Report' admin@local-
```

```
host
```

Scan files found by the find(1) command and feed infected/suspected files to the mv(1) command to move infected/suspected files to /var/quarantine directory. Any errors occured during the scan are mailed to admin@localhost.

```
      $ (find /mnt/smbshare -type f | fsav
--short --input | \
         xargs -n 1 --replace mv {} /var/
quarantine) 2>&1 | \
         mail -e -s 'FSAV Error Report'
admin@localhost
```

Check fsav, fsavd, scan engine and database versions:

```
        $ fsav --version
```

Notes

Nested archives may cause scan engine failures, if the archive scanning is enabled. The `--maxnested` option may be used to limit nested archive scanning and to prevent scan engine failures. The amount of nested archives that can be scanned without scan engine failures depend on archive types. For example, .ZIP archives containing only other .ZIP archives can be nested up to 29 archives.

The archive scanning consumes memory and scanning big archives takes lot of time during which fsavd process can not process other scan tasks. The recommended method to scan

archives is to use `--scantimeout` -option and in case the timeout occurs, the archive is scanned with a separate fsavd instance.

Bugs

Please refer to 'Known Problems' -section in release notes.

Authors

F-Secure Corporation

Copyright

Copyright (c) 1999-2006 F-Secure Corporation. All Rights Reserved.

Portions Copyright (c) 2001-2006 Kaspersky Labs.

See Also

dbupdate(8), fsavd(8)

For more information, see F-Secure home page.

fsavd

F-Secure Anti-Virus daemon

`fsavd` *options*

DESCRIPTION

`fsavd` is a scanning daemon for *F-Secure Anti-Virus*. In the startup it reads the configuration file (the default configuration file or the file specified in the command line) in the startup and starts to listen to connections to the UNIX domain socket specified in the configuration file. By default, `fsavd` forks itself into the background.

By default, `fsav` launches `fsavd` automatically if fsavd is not running. When fsavd is launched by the fsav client, fsavd terminates automatically after 30 seconds of idle time, when no client has connected to fsavd during that time.

If you want `fsavd` to stay loaded in the memory, start fsavd using the `<installdir>/etc/fsavd` startup script. It is recomended that you run fsavd as a non-priviledged user like fsav. The script can be installed under the `init.d` directory.

OPTIONS

fsavd reads option values from the policy / configuration file and from the command line. Options given from the command line override the policy / configuration file settings.

Default options or policy / configuration file options can be

overridden from the command line with the following command line options:

`--config={file[:PATH]|fsma[:OID]}` `file`: Use the configuration file based management method optionally using PATH as the configuration file instead of the default configuration file (`/etc/opt/f-secure/fssp/fssp.conf`).

`fsma`: Use the F-Secure Policy Manager based management method optionally specifying the OID used in sending alerts.

`--databasedirectory=`*`path`* Read virus definition databases from the directory *`path`*. The default is `"."`.

`--enginedirectory=`*`path`* Load scan engines from the directory *`path`*. The default is `"."`.

`--pidfile=`*`path`* Create a file containing the process identifier and remove it on the normal exit. Without this option, no pid file is created. If path is not specified, `/var/opt/f-secure/fssp/run/fsavd.pid` is created. If path specifies a relative pathname, `/var/opt/f-secure/fssp/run/path` is created. If path specifies an absolute pathname, file with that path is created.

`--socketname=`*`path`* Use the socket specified in the path.

The default is "/tmp/.fsav-<UID>".

If the file exists and is a socket, the file is removed and new socket is created. The file removal shuts down all existing fsavd instances.

If the path contains non-existing directories, the directories are created and the directory permission is set to read/write/exec permission for owner and read/exec permission for group and others. Created directories will have sticky bit on by default. Directory permissions can be changed with `dirmode` configuration file option.

Socket file permissions are set to read and write for the owner, if the daemon is started in the stand-alone mode. If the daemon is started as a daemon, the read and write permissions are also given for the group. The setting is affected by the current umask. The socket mode can be changed with the `socketmode` option from policy settings.

`--avpriskware[={on,off,yes,no,1,0}]` Enable/disable riskware scanning with the AVP scan engine (in selected products).

`--standalone` Start in the stand-alone mode. fsavd terminates automatically after a period of idle time. The option causes fsavd to

send an alarm signal to the parent process when the socket is ready to accept connections. When the option is used, fsavd does not fork(2) itself during the launch.

The option is intended to be used with fsav when fsav automatically launches fsavd. In the normal use the option can be ignored.

`--nodaemon` Do not fork program into the background.

`--help` Show command line options and exit.

`--version` Show *F-Secure Anti-Virus* version and dates of signature files, and exit.

LOGGING

fsavd logs scan failures, infected and suspected files to the fsavd's log file defined with the `logfile` fsavd writes errors during start-up to standard error stream. After successful start-up log entries are written to a log file. Error messages listed in errors section are also logged in addition to the following activity log entries:

Failed to scan file <*file path*>: <*error message*> [<*scan engine*>]

Explanation: The scan engine reports it failed to scan the file. The error message contains the reason for the failure.

Failed to scan file <*file path*>: Time limit exceeded.

Explanation: fsavd reports that the file scan failed because the scan time limit is exceeded.

Failed to scan file <*file path*>: Scan aborted.

Explanation: fsavd reports that the file scan failed because the scan was aborted. The scan is aborted if the client disconnects.

File <*file path*> disinfected.

Explanation: fsavd reports that one of the scan engines disinfected the file successfully.

File <*file path*> disinfect failed.

Explanation: fsavd reports that all the scan engines failed to disinfect the file.

File <*file path*> infected: <*infection name*> [<*scan engine*>]

Explanation: The scan engine reports that the file was found infected.

File <*file path*> contains suspected infection: <*infection name*> [<*scan engine*>]

Explanation: The scan engine reports that the file contains a suspected infection.

WARNINGS

Unknown action '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `action` in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and set the `action` field to one of the following: `disinfect`, `rename` or `delete`. The user has to restart fsavd to take values in effect.

Configuration file <*file path*> has invalid syntax at line <*line number*>

Explanation: The configuration file parsing has failed because of invalid syntax.

Resolution: fsavd tries to proceed and probably encounter some other error later. The user has to edit the configuration file and restart fsavd.

Illegal archive scanning value '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `archivescanning` field in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit configuration file and set the `archivescanning` field to one of the following: `1, 0, on, off, yes`, or `no`. The user has to restart fsavd to take values in effect.

Illegal MIME scanning value '<*user given value*>' in

configuration file <*file path*> line <*line number*>

Explanation: The `mimescanning` field in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit configuration file and set the `mimescanning` field to one of the following: `1, 0, on, off, yes`, or `no`. The user has to restart fsavd to take values in effect.

Illegal scan executables value '<*user given value*>' in configuration file <*file path*> line <*line number*>

Explanation: The `scanexecutables` field in the configuration file has an incorrect value.

Resolution: The user has to edit configuration file and set the `scanexecutables` field to one of the following: `1, 0, on, off, yes`, or `no`. The user has to restart fsav to take values in effect.

Scan extensions list is too long in configuration file <*file path*> line <*line number*>, list is truncated.

Explanation: The `extensions` field in the configuration file is more than 4096 bytes long.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and try again.

Scan timeout value '<*user given value*>' is not

valid in configuration file <*file path*> line <*line number*>

Explanation: The `scantimeout` field in the configuration file is not a valid number.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Scan timeout value '<*user given value*>' is out of range in configuration file <*file path*> line <*line number*>

Explanation: The `timeout` field in the configuration file is less than zero or more than LONG_MAX.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Maximum nested archives value '<*user given value*>' is not valid in configuration file <*file path*> line <*line number*>

Explanation: The `maxnestedarchives` field in the configuration file is not a number.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Maximum nested archives value '<*user given value*>' is out of range in configuration file <*file path*> line <*line number*>

Explanation: The `maxnestedarchives` field in the configuration file is less than zero or more than LONG_MAX.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Maximum scan engine instances value '<*user given value*>' is not valid in configuration file <*file path*> line <*line number*>

Explanation: The `engineinstancemax` field in the configuration file is not a number.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and try again.

Maximum scan engine instances value '<*user given value*>' is out of range in configuration file <*file path*> line <*line number*>

Explanation: The `engineinstancemax` field in the configuration file is less than zero or more than LONG_MAX.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and try again.

Unknown option '<*user given option name*>' in configuration file <*file path*> line <*line number*>

Explanation: The configuration file contains an unknown option name.

Resolution: fsavd tries to proceed. The user has to edit the configuration file and restart fsavd.

Unknown syslog facility '<*user given value*>' in configuration file <*file path*> line <*line

number>

Explanation: The `syslogfacility` ield in the configuration file has an incorrect value.

Resolution: fsavd tries to proceed. The user has to edit configuration file and set the `syslogfacility` field to one of the facility names found in syslog(3) manual page. The user has to restart fsavd to take values in effect.

<engine name> scan engine seems to be dead.

Explanation: The scan engine <engine name> has died. Either the timeout occured during the file scan or the scan engine process has died unexpectly.

Resolution: fsavd has noticed the scan engine has died. fsavd tries to restart the scan engine. If the scan engine was scanning a file, the file is reported to be failed to scan.

Database file <*file path*> not needed and should be deleted.

Explanation: The scan engine reports that the database directory contains a depracated database file.

Resolution: The message is only informational. The user may delete the file in path <*file path*>.

Database file <*file path*> is missing.

Explanation: The scan engine reports that the database file <*file path*> is missing from the database directory.

Resolution: The scan engine fails to start. fsavd will tries to

restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

Database file <*file path*> is not a valid database.

Explanation: The scan engine reports that the database file <*file path*> is not a valid database file in the database directory.

Resolution: The scan engine fails to start. fsavd tries to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

Database file <*file path*> is not a database file.

Explanation: The scan engine reports that the database file <*file path*> is not a valid database file in the database directory.

Resolution: The scan engine fails to start. fsavd tries to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start scan engine automatically.

Database file <*file path*> is corrupted.

Explanation: The scan engine reports that the database file <*file path*> is not a valid database file in the database directory.

Resolution: The scan engine fails to start. fsavd tries to

restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

Database file <*file path*> has wrong database version.

Explanation: The scan engine reports that the database file <*file path*> has an incorrect version.

Resolution: The scan engine fails to start. fsavd tries to restart the scan engine. The user needs to perform database update and possibly restart fsavd if fsavd fails to start the scan engine automatically.

<engine name> scan engine initialization time limit exceeded, going for shutdown.

Explanation: The scan engine has exceeded its initialization time limit (300 seconds). The reason may be a high system load and thus the scan engine processes do not get enough processing time to load the databases. Furthermore, the hardware failure may cause the scan engine to hang while reading the databases.

Resolution: fsavd shuts down the scan engine process and tries to restart the scan engine. If problem still occurs, the user may try to update databases or scan engine to resolve the problem. If the problem persists the user needs to contact F-Secure support.

<engine name> scan engine inactive for too long, going for shutdown.

Explanation: The scan engine is not responding to the keep-alive messages and it has not reported scan nor initialization statuses for a limited time period (300 seconds). The problem may be in a file which the scan engine is scanning. If the user can recognize the source as a problematic file, the user should make a bug report and send a file sample to F-Secure.

Resolution: fsavd shuts down the scan engine process and restarts the scan engine.

Could not open logfile <*file path*>: <*OS error message*>

Explanation: fsavd failed to open the logfile <*file path*> for logging.

Resolution: fsavd writes logs to default logfile (stderr). The user may reconfigure the logfile location and restart fsavd.

Cannot change working directory to '<*file path*>'.

Explanation: fsavd failed change working directory database directory.

Resolution: fsavd tries to continue using the current directory as working directory.

ERRORS

Failed to open scan engine shared library.

Explanation: fsavd cannot find required scan engine shared library files which are normally found from <*install directory*>/*lib*.

Resolution: fsavd exits with error status. Installation or engine directory in configuration file maybe incorrect or `--engine-directory` command-line option has incorrect path.

`Failed to load required symbol from scan engine library.`

Explanation: fsavd finds required scan engine shared library files but fails to load correct library calls from the library.

Resolution: fsavd exits with error status. Scan engine shared libraries are corrupted. Product needs to be re-installed.

`Options parsing failed.`

Explanation: The user has given an unknown option or an option value from the command-line.

Resolution: fsavd exits with error status. The user has to correct the command-line parameters and start fsavd again.

Database directory '*<directory path>*' is not valid in configuration file at line *<line number>*: *<OS error message>*

Explanation: The user has entered a database directory path which either does not exist, is not accessible or is too long from the configuration file.

Resolution: fsavd exits with error status. The user has to correct the path and start fsavd again.

Database directory '*<directory path>*' is not valid: *<OS error message>*

Explanation: The user has entered a database directory path which either does not exist, is not accessible or is too long from the command-line.

Resolution: fsavd exits with error status. The user has to correct the path and start fsavd again.

Database update directory '<*directory path*>' is not valid in configuration file at line <*line number*>: <*OS error message*>

Explanation: The user has entered a database update directory path which either does not exist, is not accessible or is too long from the configuration file.

Resolution: The user has to correct the path and start fsavd again.

Scan engine directory '<*directory path*>' is not valid in configuration file at line <*line number*>: <*OS error message*>

Explanation: The user has entered a scan engine directory path which either does not exist, is not accessible or is too long from the configuration file.

Resolution: fsavd exits with error status. The user has to correct the path and start the fsavd again.

Scan engine directory '<*directory path*>' is not valid: <*OS error message*>

Explanation: The user has entered a scan engine directory path which either does not exist, is not accessible or is too

long from the command-line.

Resolution: fsavd exits with error status. The user has to correct the path and start the fsavd again.

Could not open configuration file <*file path*>: <*OS error message*>

Explanation: The configuration file path given from the command-line, the file does not exist or it is not accessible.

Resolution: fsavd tries to proceed and probably encounters some other error later. The user has to create the configuration file to the default path or give the correct path to an accessible configuration file and restart fsavd.

Access to database index file '<*file path*>' failed: <*OS error message*>

Explanation: The database directory path (set in the configuration file or from the command-line) is not correct and the daemon cannot find the `dbindex.cpt` file.

Resolution: fsavd exits with error status. The user has to give the correct database path and start fsavd again.

stat for database index file failed: <*path to dbindex.cpt*>

Explanation: The database directory path (set in the configuration file or from the command-line) is not correct and fsavd cannot find the `dbindex.cpt` file.

Resolution: fsavd exits with error status. The user has to give the correct database path and start fsavd again.

accept failed because run out of memory.

Explanation: The accept(2) has failed because system ran out of the memory.

Resolution: fsavd exits with error status. The user has to free some memory and start fsavd again.

FILES

`/etc/fssp.conf` The default configuration file for *F-Secure Anti-Virus*

`$HOME/.fssp.conf` User specific configuration file for *F-Secure Anti-Virus*

`<install directory>/etc/fsav` Startup file for *F-Secure Anti-Virus*

`<install directory>/databases` Directory for Anti-Virus signature database files.

`<install directory>/lib` Directory for Anti-Virus scan engine and *F-Secure Anti-Virus* shared library files.

EXAMPLES

Start fsavd as a background daemon process using the default configuration file:

```
$ fsavd
```

Start fsavd as a foreground process using the default configu-

ration file:

```
$ fsavd --nodaemon
```

Start fsavd as a background daemon process using 'fsav-test.conf' as a configuration file:

```
$ fsavd --configfile=fsav-test.conf
```

Check fsavd, scan engine and database versions:

```
$ fsavd --version
```

Bugs

Please refer to 'Known Problems' -section in release notes.

AUTHORS

F-Secure Corporation

Copyright

Copyright (c) 1999-2006 F-Secure Corporation. All Rights Reserved. Portions Copyright (c) 2001-2006 Kaspersky Labs.

SEE ALSO

dbupdate(8), fsav(1), fssp.conf(5)

For more information, see F-Secure home page.

dbupdate

Virus definition database update for *F-Secure Anti-Virus*

`dbupdate` --help --auto *directory*

PARAMETERS

`--help`	Show the short help of command line options and exit.
`--auto`	Do not download databases synchronously but update databases previously downloaded by F-Secure Automatic Update Agent. Used for fully automatic database updates.
`directory`	Do not update databases downloaded by F-Secure Automatic Update Agent, update from the specified directory instead.

DESCRIPTION

`dbupdate` is a shell script for updating *F-Secure Anti-Virus* Virus Definition Databases. It can update databases downloaded by F-Secure Automatic Update Agent (a fully automatic background process) or databases transferred to the host by other means (such as ftp). Before databases are updated, `dbupdate` performs the necessary validation for databases to prevent any corrupted or tampered databases to be taken into use.

ON DEMAND UPDATE OVER NETWORK

Use the `dbupdate` command (without any parameters) if there is a need to check new database updates immediately over the network and take new databases into use.

SCHEDULED UPDATE OVER NETWORK

Typically, dbupdate is started from cron(8) frequently with the following command: `dbupdate --auto`. This takes into use updates that F-Secure Automatic Update Agent has the previously downloaded.

OPERATION

If new databases are available, database files are copied to `updatedirectory`. Database files are then validated using `daastool` and `dbtool`. After the validation, database files are copied to `databasedirectory` using the `fsav --dbupdate=updatedirectory` command.

ERROR CODES

If update with `F-Secure Automatic Update Agent` fails, an error message

```
Database update failed. Error code: XX
```

with one of the following errorcodes will be printed:

`2`	Connection to AUA daemon timed out. Try restarting AUA daemon.
`30`	Could not connect to AUA daemon. Perhaps AUA daemon is not running.

`50`	Could not copy update. Copying database update failed, probably because lack of free disk space.
`51`	Could not extract update. Extracting database update failed, probably because lack of free disk space.

EXIT VALUE

`0`	Nothing was updated since no new updates were available.
`1`	An error has occurred. See program output and `/var/opt/f-secure/fssp/dbupdate.log` for details.
`2`	Virus definition databases were successfully updated.

BUGS

Please refer to 'Known Problems' section in the release notes.

AUTHORS

F-Secure Corporation

Copyright

Copyright (c) 1999-2006 F-Secure Corporation. All Rights Reserved.

SEE ALSO

fsav(1) and fsavd(8)

For more information, see F-Secure home page.

fsfwc

command line interface for firewall daemon

`fsfwc` *options*

Description

With this tool firewall can be set to different security levels.

If invoked without any options, it will show current security level and minimum allowed.

Options

`--mode`

`{block,server,mobile,office,strict,normal,bypass}` Will set firewall to requested security level if allowed by minimum security level setting.

`block` Won't allow any packets to go in or out (excluding the loopback interface)

`server` Will allow only IP configuration via DHCP, DNS look-ups and ssh protocol out and IN

`mobile`	Profile for roadwarriors: ssh and VPN protocols are allowed. DHCP, HTTP, FTP and common email protocols are allowed. All incoming connections are blocked.
`office`	Profile for office use. It is assumed that some external firewall exists between Internet and the host. Any outgoing TCP connections are allowed. A rule to allow Windows networking inside the same network is included but is not enabled by default.
`strict`	Very much like the mobile profile, except it does not allow DHCP.
`normal`	All outgoing connections are allowed. All incoming con-

	nections are denied.
`bypass`	Allow everything in and out.

RETURN VALUES

fsfwc has the following return values.

```
0Normal exit;
1Error occurred.
```

AUTHORS

F-Secure Corporation

COPYRIGHT

Copyright (c) 1999-2006 F-Secure Corporation. All Rights Reserved.

SEE ALSO

For more information, see F-Secure home page.

fsic

Command line interface for integrity checker

`fsic` *options target ...*

Description

F-Secure Integrity Checker will monitor system integrity against tampering and unauthorized modification.

If invoked without any options, `fsic` will verify all files in the known files list and report any anomalies.

Options

`-V, --verify` *`[options]`* Default operation if invoked without any options. Verify the system and report any deviations against baselined information.

`--show-all` Enable listing of all files in the baseline (by default only files which do not match baselined information are shown)

`--show-details` Enable full listing of file signatures.

If nothing has

changed, only baselined inode information is shown.

If file differs from baselined information, detailed comparison is shown.

`--virus-scan={yes=default,no}`

Scan for viruses when verifying. (default: yes)

`--ignore={attr,hash}` Ignore specified file properties if they differ from the baseline information. Only attr or hash can be specified at a time, not both. (default: nothing is ignored)

`--auto={yes,no=default}` Disable action confirmation. Assumes 'Yes' to all enabled actions. Please note that --auto=no disables the auto switch, same as if --auto would not have

been given at all. (default: no)

`-v, --verifyfile` *`[options]`* This mode will validate only files given from command line OR stdin. This option has the same sub-options as verify.

`-B, --baseline` *`[options]`* Calculate baseline information for all of the files. If a previous baseline already exists, it will be overwritten.

`--virus-scan=`*`{yes=default,no}`*

Enable/disable virus scanning of the files during baselining. Viruses are scanned with options --dumb and --archive. (See fsav(1))

`--auto=`*`{yes,no=default}`* Disable the action confirmation. Assumes 'Yes' to all enabled actions. Please note that --auto=no disables the auto switch, same as if --auto would not have been given at all. (default: no)

`-b, --baselinefile` *`[options]`* This mode will add only entries given from command line OR stdin to baseline. This option has same sub-options as baseline.

`-a, --add` *`[options] target ...`* Add a target[s] to the known files list. Targets must be real files or links. By default all files are added as monitored. A new baseline needs to be generated after all file additions have been performed.

`--protect=`*`{yes,no=default}`* Add the file as protected, instead of monitored. When a file is added as protected, the file can only be opened for reading. Opening the file in write mode will fail.

`--access=`*`{allow=default,deny}`*

Specify whether file access is allowed or denied if file data or metadata does not match baselined information.

`--alert=`*`{yes=default,no}`* Specify whether to send

an alert if file differs from baselined information.

`-d, --delete` ***`target ...`*** Remove target[s] from the known files list. A new baseline needs to be generated after all file deletions have been performed.

verify action reports

If --show-all is specified, then also clean files are reported, as follows.

```
[ OK ] PRA /bin/ls
[ OK ] P.D /bin/chmod
```

Characters on second column tell how file is handled in integrity checking. P implies Protected, R is for Report (send alert for every access to this file if file differs from baselined), A is Allow access even if differs from baseline, D means that access is denied if file does not match with baselined information. '.' on either P or R column means that Protection or Reporting respectively is not enabled.

If a change is detected against the baseline, it is reported as follows

```
   [Note] .RA /bin/ls Hash does not match
baselined hash
    [Note] .RA /bin/ls inode information
does not match baselined data
```

So even if inode data is changed Hash might be same (touch on a file will change inode data) however IF hash is changed and inode data is still same then file contents has been modified and it's mtime set back to what it was with utime() (man 2 utime).

If --show-details is specified, then deviations against baseline are reported as follows

```
  [Note] ( RA) /bin/ls Hash does not match
baselined hash
   [Note] ( RA) /bin/ls inode information
does not match baselined data

mode:uid:gid:len:mtime  hash
                                        Old
81ed:0:0:31936:1096007887
e2c2f03d5460690211fa497592543371
                                        Now
81ed:0:0:31940:1096388689
08c4eae2cf02c4214ba48cb89197aa66
```

If no deviations are found and --show-all is also specified then following will be reported

```
        [    OK    ]    (    RA)    /bin/ls
(81ed:0:0:620676:1077202297)
```

baseline action reports

When --baseline is specified the integrity checker will recalcu-

late hash and inode information for all files known to the integrity checker. Previously generated baseline will be over-written.

User will be asked to confirm adding files to new baseline. For example,

```
  /bin/ls: Accept to baseline? (Yes,No,All
yes, Disregard new entries)
```

If file has been modified `fsic` will ask

```
   [Note] /bin/ls seems to differ from
baselined entry. Want to rebaseline it?
[no]
```

WARNINGS

None.

FATAL ERRORS

None.

SCAN ERRORS

None.

RETURN VALUES

fsic has the following return values.

```
        0Success. Normal exit
        1Error in invocation, baselining or
verification
```

```
2No baseline exists yet.
3System compromised.
```

Return value of 3 indicates that one or more of the following happened;

```
* Incorrect passphrase, or
* Files do not match baselined
information, or
* A virus was detected in one of the
files
```

FILES

None.

EXAMPLES

None.

NOTES

None.

BUGS

None.

AUTHORS

F-Secure Corporation

COPYRIGHT

Copyright (c) 1999-2006 F-Secure Corporation. All Rights Reserved.

SEE ALSO

For more information, see F-Secure home page.

F Technical Support

Introduction 166
F-Secure Online Support Resources 166
Web Club 167
Virus Descriptions on the Web 167

Introduction

F-Secure Technical Support is available through F-Secure support web pages, e-mail and by phone. Support requests can be submitted through a form on F-Secure support web pages directly to F-Secure support.

F-Secure Online Support Resources

F-Secure support web pages for any F-Secure product can be accessed at http://support.f-secure.com/. All support issues, frequently asked questions and hotfixes can be found under the support pages.

If you have questions about F-Secure Anti-Virus Linux Server Security not covered in this manual or on the F-Secure support web pages, you can contact your local F-Secure distributor or F-Secure Corporation directly.

For technical assistance, please contact your local F-Secure Business Partner. Send your e-mail to:
Anti-Virus-<country>@f-secure.com

Example: Anti-Virus-Norway@f-secure.com

If there is no authorized F-Secure Anti-Virus Business Partner in your country, you can submit a support request directly to F-Secure. There is an online "Web submit form" accessible through F-Secure support web pages under the "Contact Support" page. Fill in all the fields and describe the problem as accurately as possible.Please include the following information with your support request:

- Version numbers of F-Secure Anti-Virus Linux Server Security, and possibly the version numbers of F-Secure Policy Manager Server and F-Secure Policy Manager Console if you use centralized administration. Include the build number if available.
- Description how F-Secure components are configured.
- The name and the version number of the operating system on which F-Secure products and protected systems are running.
- The version number and the configuration of your servers. If possible, describe your network configuration and topology.

- A detailed description of the problem, including any error messages displayed by the program, and any other details that could help us replicate the problem.
- *Logfile* from the machines running F-Secure products.

Web Club

The F-Secure Web Club provides assistance and updated versions of F-Secure products. To connect to the Web Club directly from within your Web browser, go to:
http://www.F-Secure.com/anti-virus/webclub/corporate/

Virus Descriptions on the Web

F-Secure Corporation maintains a comprehensive collection of virus-related information on its Web site. To view the Virus Information Database, connect to:
http://www.F-Secure.com/virus-info/

www.f-secure.com